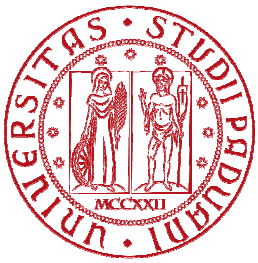


UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA INFORMATICA

TESI DI LAUREA SU PROGETTO: STUDIO DI FATTIBILITÀ PER UN SISTEMA DI IDENTITY MANAGEMENT

(Laurea triennale DM 509/99 – indirizzo Informatica)

Relatore : SERGIO CONGIU

Laureando : ENRICO BIZZARO

ANNO ACCADEMICO 2011 – 2012

INDICE

1. INTRODUZIONE:

Questo progetto prevede lo sviluppo di un sistema di Identity Management (IM) , ovvero un insieme di tecnologie in grado di consentire alle organizzazioni di facilitare - e al tempo stesso controllare - gli accessi degli utenti ad applicazioni e dati critici, proteggendo contestualmente i dati personali da accessi non autorizzati, gestendo l'intero ciclo di vita degli utenti, rendendo disponibili strumenti di password management ed essendo così funzionale alla realizzazione di meccanismi SSO (single sign-on).

Con Identity Management dunque si intende la completa gestione delle identità digitali di una persona fisica, dal processo di creazione e organizzazione, fino all'eliminazione dell'identità digitale stessa.
Ogni singola persona, dipendente di una azienda o utente esterno di un servizio, è oggetto di un processo di assegnazione di molte identità digitali che possono riguardare l'account di posta o l'accesso alla intranet aziendale, in maniera coerente con il suo specifico ruolo aziendale.

Nell' Identity Management ciascuna di queste identità digitali va attivata (Provisioning) e disattivata (deProvisioning) in maniera coerente alle politiche aziendali e in modo automatico per evitare errori o ritardi. Ad esempio, nel caso di licenziamento di un dipendente, l'intero processo di disattivazione dei suoi account deve essere eseguito nel modo più rapido ed efficace possibile.
Processi ripetitivi possono essere facilmente eliminati riducendo notevolmente i costi operativi di gestione delle identità digitali grazie all'automazione di processi e servizi self service, ne sia un esempio il processo di rigenerazione di una password smarrita.

Le soluzioni di Identity Management, spesso associate ad architetture basate su Single Sign On (SSO), rendono molto più sicura ed efficiente una infrastruttura di servizio eliminando le problematiche di autenticazione e autorizzazione.

Infine, la possibilità di effettuare auditing e monitoraggio sulle attività di ogni identità digitale, consente di mettersi al riparo da impiegati fraudolenti o furti di identità, consentendo una maggior aderenza alle politiche di sicurezza aziendale e, quando necessario, un più facile percorso di certificazione. L'azienda può infatti conoscere in ogni momento "chi fa cosa".

Il progetto realizzato per un ente pubblico, il comune di "Cavarzere", prevede la gestione del "ciclo di vita" delle identità digitali mediante il confronto delle principali tecnologie presenti nel mercato nel contesto richiesto al fine di cercare un prodotto il più possibile adatto alle esigenze del cliente.

2. SOCIETÀ:

La SAIES srl, nasce nel 2001 come somma delle competenze acquisite da un gruppo di informatici professionisti che hanno maturato la loro esperienza pluriennale sia all'interno dell'ente pubblico, sia presso aziende informatiche il cui prodotto è prettamente indirizzato alla gestione delle amministrazioni locali e delle medie aziende.
Questo consente alla società di operare con un elevata specializzazione e professionalità in rapporto alle problematiche della pubblica amministrazione, soddisfacendo alle specifiche esigenze d'ogni settore.

Lo scopo della SAIES srl è quello di mettere a frutto la propria esperienza per fornire assistenza e servizi informatici ad ogni livello.
Inoltre, la società è in grado di offrire una mirata consulenza sui progetti e le strategie informatiche che un'azienda o la Pubblica Amministrazione intendono attuare.
I servizi offerti dall'azienda partono dal lato hardware e vanno fino al lato software, una copertura a 360 gradi su quelle che sono le esigenze del cliente.
Esempio di ciò che viene svolto all'interno dell'azienda sono progettazione ed installazione di reti e sistemi informatici di medio grandi dimensioni, progetti volti a soddisfare i desideri del cliente e a perseguire la massima affidabilità e sicurezza dei sistemi che verranno realizzati.

L'azienda fornisce inoltre la possibilità di installazione, previa progettazione, di cablaggi strutturati di qualità, dotati di opportuni dispositivi di protezione per la corrente elettrica onde consentire la disponibilità ed il corretto funzionamento di tutti gli apparati elettrici.
Per garantire il raggiungimento di questi obiettivi, la SAIES srl si avvale, oltre che delle proprie risorse umane, anche della collaborazione di aziende altamente specializzate nel settore di interesse.

L'azienda assicura un lavoro effettuato con puntualità, professionalità e cordialità per ottenere un rapporto di soddisfazione reciproco con i clienti.
Al proprio interno, essa gestisce e personalizza alcuni dei software richiesti dal cliente per garantire allo stesso una maggiore flessibilità del sw ed un utilizzo che sia conforme alle esigenze.
Il personale qualificato all'interno dell'azienda è in grado di tenere eventualmente dei corsi di formazione per coloro che necessitano di tale servizio, ad esempio nel momento di installazione di un nuovo software vengono formati, a richiesta, sia le utenze che il personale preposto all'amministrazione di tale programma.

L’azienda fornisce un servizio di supporto giornaliero per tutte le aziende od enti che ne necessitano, effettuando l’ordinaria manutenzione sia dal lato software che da quello hardware. Vengono infatti controllati giornalmente i risultati dei backup dei clienti in modo da garantire sempre la ridondanza dei dati ed evitare la perdita di dati sensibili.
Lavorando anche con enti pubblici, l’azienda ha sviluppato in tal senso dei sistemi atti a garantire la continua disponibilità dei dati; alcune tipologie di dati trattati infatti, come quelli anagrafici, richiedono una particolare cura data la sensibilità degli stessi.

L’azienda vanta inoltre la capacità di aver sensibilizzato alcuni enti pubblici sull’importanza dei database, e negli anni, di aver messo in sicurezza tutte quelle strutture che si rivelavano deboli ed a rischio nel caso si fossero verificate situazione / eventi naturali ritenute improbabili ma pur sempre possibili.

Il mio lavoro all’interno dell’azienda si è sempre svolto in un clima di professionalità e serenità che mi ha consentito di svolgere i miei compiti in tutta sicurezza e tranquillità.
Alcuni dubbi e/o incertezze che ho incontrato durante lo svolgimento di questo stage sono stati prontamente risolti grazie alla competenza del mio tutor, il quale mi ha fatto apprezzare ciò che stavo facendo e ciò che quotidianamente tutto il team svolge.
Ho potuto inserirmi nell’ambiente lavorativo ed osservare da vicino una realtà aziendale abbastanza vasta che ricopre diverse aree di interesse, vedere all’opera e confrontarmi con professionisti del settore dai quali ho imparato molto sia a livello tecnico sia a livello umano.

3. LAVORO SVOLTO:

Il lavoro è iniziato con un approfondimento sull'argomento d'interesse, avvalendomi degli studi di fattibilità già realizzati dall'azienda e degli strumenti messi a disposizione dalla tecnologia attuale.

Ho cominciato lo studio con un'analisi degli obiettivi che ci sono stati forniti con il successivo svolgimento della fase di "analisi delle esigenze".
In questa fase di studio ho utilizzato più metodi per ottenere un'analisi il più possibile precisa ed affidabile di ciò che ci è stato richiesto.
Ho poi reperito informazioni utilizzando il materiale che le varie strutture, per le quali verrà progettato il sistema, ci avevano gentilmente messo a disposizione per far capire il quadro d'interesse iniziale.
Mi sono inoltre avvalso dell'uso di grafici e schemi UML per la descrizione delle esigenze di dati e dei processi che coinvolgono utili ai fini dello studio di fattibilità.
La determinazione delle esigenze funzionali è un aspetto molto importante poiché questo prevede un analisi più approfondita di quello che si andrà a creare.
Nel mio caso, uno sviluppo di un sistema che dia la possibilità all'utente di accedere al sistema con un livello di autorizzazione garantito dal proprio ruolo interno, il che è molto importante per preservare e garantire la sicurezza e l'integrità dei dati.

La valutazione della situazione di partenza è anch'essa molto importante poiché ci permette di capire con quale contesto dovremo inizialmente interfacciarci, nel nostro caso le strutture non hanno al loro interno sistemi simili che permettano l'identificazione degli utenti a seconda del ruolo da loro ricoperto.

Il comune di Cavarzere vede varie sedi collocate in tutto il territorio comunale e collegate tra di loro attraverso rete pubblica e/o privata, che facilita la comunicazione e lo scambio di informazioni tra di loro.
Un'analisi della tecnologia già esistente può facilitare la creazione e lo sviluppo del sistema, usufruendo anche delle risorse già presenti, per minimizzare e costi ed aumentare l'efficienza.

Una volta approfondita la conoscenza sulla struttura e la situazione interna, si è svolto un lavoro di ricerca ed analisi delle soluzioni presenti all'interno del mercato per poterne poi effettuare una valutazione d'insieme.
Queste soluzioni già esistenti, unite a quella su realizzazione in-house, in questo caso non realizzabile perché non sono disponibili le risorse interne necessarie, ed ad una realizzazione su commessa esterna, che preveda la realizzazione da 0 del software con tempi di

realizzazione necessariamente lunghi ma con un livello di personalizzazione che dovrebbe soddisfare tutte le richieste del cliente poiché è stato creato appositamente per quest'ultimo, danno un quadro delle varie alternative possibili.

Molto importanti sono poi i vincoli imposti da nostro cliente che vanno da quelli economici con un tetto di spessa massima che in questo caso non devo superare i 50000 euro a quelli temporali in cui è previsto che il tempo per lo sviluppo e l'avviamento del sistema non debba superare i 18 mesi.
Non sono inoltre da trascurare ovviamente anche come vincolo per una scelta corretta come sopra citato le tecnologie già esistenti quali ad esempio licenze di database già acquisite, onde evitare di acquistarne di nuove e ridurre così l'impatto organizzativo e di conseguenza anche la spesa finale.

Tutto ciò è stato poi trattato nelle "considerazioni" all'interno dello studio di fattibilità in cui vengono fatte delle valutazioni iniziali sulle diverse tipologie di soluzioni presenti all'interno del mercato, cha vanno da quelle FOSS ovvero prodotti che sono Open Source, con vari vantaggi legati appunto al fatto di essere OS e altri svantaggi che ne derivano conseguentemente, alle soluzioni a pagamento già sviluppate da altre aziende (Novell, IBM, Oracle) alla soluzione su commessa esterna, la soluzione che precedentemente avevo citato tra le possibili ovvero in- house è stata scartata a priori perché non si ha la possibilità di realizzare una tale soluzione.
Altre considerazioni sono poi state fatte sui vincoli che ci sono stati imposti e/o dalle normative vigenti, la privacy infatti in questo caso è molto importante, trattando questo sistema dati sensibili e personali di ogni utente, infatti si vuole e si deve garantire che queste informazioni rimangano riservate e che non vengano divulgate senza l'autorizzazione della persona interessata.

All'interno dello studio di fattibilità vengono poi create le varie ipotesi di soluzione e solo quelle ritenute più opportune vengono sviluppate.
Per effettuare le valutazioni necessarie si è realizzato una base di componenti hardware comuni alle varie soluzioni a cui aggiungere poi la soluzione software che sarà reputata più conveniente.
I dati delle utenze sono già presenti all'interno di un database con il quale ci si dovrà interfacciare per popolare la nostra base di dati e riuscire poi ad utilizzare il nostro sistema.
Per quanto le difficoltà all'uso del sistema possano essere minime, è pur sempre possibile commettere errori di utilizzo, quindi è necessario formare gli utenti che andranno ad utilizzare il sistema per un corretto uso dello stesso , al fine di evitare malfunzionamenti dovuti ad un non corretto utilizzo dello strumento.

Come tutti i programmi anche questo dovrà sostenere una fase di test, un necessario un periodo di prova nella quale testare il corretto funzionamento del sistema installato.
Tutto ciò è valido in linea di massima per i pacchetti già presenti nel mercato, invece se il software viene realizzato ex-novo, su commessa esterna, i tempi di realizzazione si dilateranno, rispetto a quelli di personalizzazione, le fasi di test dovranno ad esempio essere più lunghe ed approfondite (alpha e beta test).

Analizzando le soluzioni proposte la soluzione su commessa esterna presenta un rischio troppo elevato dettato da un lungo periodo di sviluppo, collaudo, avvio del software e per la formazione non solo degli utenti ma anche dei tecnici interni addetti alla gestione del sistema informativo, per questo ed altri motivi perciò è stata scartata. Sebbene i pacchetti software necessitino di una personalizzazione, si presentano comunque come software già pienamente testati, molto completi e ben flessibili che si adattano bene alle varie esigenze che possono insorgere nelle varie strutture. La scelta sarà quindi orientata verso il pacchetto applicativo. Tra le varie opzioni troviamo anche la soluzione Open Source offerta dalla Sun, grande azienda produttrice di software di elevata qualità, che in parte troviamo oramai in quasi tutti i nostri computer (Suite Java): oltre a questo vi sono anche le soluzioni di Novell e IBM. La nostra scelta, dopo aver effettuato un confronto delle varie caratteristiche e dell'analisi del rischio cade su IBM, ritenendo l'azienda una delle migliori in questo campo con un software assolutamente completo e all'avanguardia nel settore. Essendo quindi la scelta di IBM l'unica realmente realizzabile e sicura per il nostro cliente si procede con l'analisi nel dettaglio di questa soluzione.
Da qui ho sviluppato il progetto di massima per la soluzione ritenuta più adatta.
Con la definizione degli obiettivi, delle funzionalità del sistema scelto e la valutazione delle componenti hardware ottimali per questo tipo di pacchetto, infatti si devono garantire oltre alle risorse minime indispensabili per il funzionamento del software stesso anche delle caratteristiche che consentano la scalabilità, la possibilità di essere durevole nel tempo garantendo prestazione consone al proprio utilizzo.
Deve essere inoltre garantita l'affidabilità garantendo un elevata disponibilità dei dati con apposite ridondanze in credo di soddisfare le esigenze di applicazione business - critical e mission - critical.

Il sistema inoltre necessita di interventi manutentivi periodici, poiché deve essere assicurata l'efficienza e la funzionalità del sistema. Possono essere previsti degli interventi su software dovuti a modifiche ad esempio a vincoli normativi i quali impongono il cambiamento di un parte del sistema. La flessibilità di questo software permette di eseguire le modifiche senza dover interpellare la ditta produttrice.

Per la sicurezza dei dati contenuti all'interno del database, questi devono essere soggetti a copie di back-up per eliminare eventuali possibilità di perdita.
Per fare ciò sono state studiate delle soluzione "ad hoc " che consentono l'archiviazione sicura delle informazioni sensibili presenti, con soluzioni che prevedono anche, nel caso fosse necessario, la cosiddetta sostituzione a caldo "hot swap" degli hard disk se uno di questi si fosse guastato ed il cui contenuto poi verrà ripristinato.

E' stato creato poi un piano di realizzazione del sistema che si svolge nelle seguenti fasi:

A) Acquisto del prodotto e personalizzazione;
B) Installazione;
C) Migrazione dati;
D) Formazione utenti;
E) Periodo di prova.

Il tempo totale previsto per rendere operativo il sistema è stato valutato in 12 mesi, tempo che soddisfa pienamente i 18 mesi precedentemente indicati nei vincoli.

La realizzazione di questo sistema di identity management comporta un reale cambiamento al modus operandi fin'ora adottato. Innanzitutto tutte le operazioni che prima venivano eseguite su carta come la registrazione di un nuovo utente e dei suoi relativi dati viene ora eseguito a computer, alla fine della quale verrà creato un nuovo account con assegnato il ruolo che ricoperto dal nuovo utente e i relativi privilegi assegnati.
Inoltre tutte le operazioni di accesso ai dati saranno ora per via telematica. Non ci sarà più bisogno di particolari autorizzazioni firmate dai responsabili per poter accedere ai documenti del tipo progetti, schemi, tabelle di codici o altro, il controllo della effettiva possibilità di reperire informazioni sensibili verrà automaticamente verificato dal sistema dopo aver effettuato la procedura di login.
Quindi tutte quelle operazioni che richiedevano delle autorizzazioni per compiere una qualsiasi attività come ad esempio la formale richiesta delle ferie o l'invio di un certificato medico o ancora la timbratura del cartellino verranno eseguite e controllate in modo automatico e inoltrate direttamente a quelle figure le quali hanno il potere di poter accettare, modificare o rifiutare tale richiesta con dei sistemi di Workflow personalizzati.
Tutto ciò evidentemente avrà un impatto sull'organizzazione per cui è necessario un periodo di 180 giorni di avvio in parallelo con il vecchio sistema.
Ovviamente il sistema porterò dei benefici all'interno che sono stati tutti trattati all'interno dello studio di fattibilità ed un'attenta analisi dei costi/benefici sarà ciò che si spera indurrà il nostro cliente ad approvare il progetto.
Poi ampiamente trattati nello studio.

4. STUDIO DI FATTIBILITA': IDENTITY MANAGEMENT

4.1. OBIETTIVI DELLO STUDIO

4.1.1. Descrizione degli obiettivi

Con **Identity Management (IM)** si intendono i sistemi integrati di tecnologie, criteri e procedure in grado di consentire alle organizzazioni di facilitare - e al tempo stesso controllare - gli accessi degli utenti ad applicazioni e dati critici, proteggendo contestualmente i dati personali da accessi non autorizzati, gestendo l'intero ciclo di vita degli utenti, avere strumenti di password management ed essere quindi funzionale alla realizzazione di meccanismi SSO (single sign-on).
Il progetto consiste nell'analisi e definizione del sistema di Identity Management più adatto per l'ente, confrontando le principali tecnologie presenti nel mercato (Tivoli Identity Manager di IBM, Identity Manager di Novell, Sun Identity Management di Sun Microsystems, ecc.).
L'obiettivo sarà la definizione ed implementazione di un modello di sistema IM da applicare a tutte le strutture dislocate nel territorio comunale.

4.1.2. Riferimenti al piano di sviluppo del S.I.

Non sono stati rilevati altri piani di sviluppo di un sistema di Identity Management per il sistema informativo richiesto.

4.2. ANALISI DELLE ESIGENZE

4.2.1. Descrizione dei metodi usati

Per l'analisi delle esigenze abbiamo utilizzato più metodi per ottenere un'analisi il più possibile precisa ed affidabile di ciò che il committente richiede.
Per reperire informazioni abbiamo utilizzato il materiale riguardante l'ente reperito tramite web ed altro già in nostro possesso. Ci si è inoltre avvalsi dell'uso di grafici e schemi UML per la descrizione delle esigenze dei dati e dei processi che coinvolgono lo studio di fattibilità.

Analisi dei processi

L'ente è organizzato in 9 sedi, presenti tutte all'interno dell'area comunale
All'interno dell'ente sono presenti diverse aree di interesse che vanno dalle varie sedi comunali alla biblioteca, asilo nido e scuole .

Analisi dei fattori critici

Nella seguente analisi andremo a determinare quali siano i fattori critici nella realizzazione del sistema, suddividendoli in due categorie: fattori critici per l'organizzazione ed individuali.

FATTORI CRITICI DELL'ORGANIZZAZIONE

1. Conformità alle norme e regole della legge anche per quanto riguarda la sicurezza.

Il trattamento dei dati sensibili devono seguire i criteri minimi di protezione previsti dalla legge

2. Fornire un sistema semplice veloce e sicuro per l'accesso degli utenti.

Il sistema dovrà essere di semplice utilizzo e usufruibile da tutti gli utenti che in caso di bisogno dovranno essere supportati da un servizio di assistenza.

3. Elevata disponibilità e integrità dei dati.

Il sistema dovrà assicurare la disponibilità dei dati con meno interruzioni possibili, consentite solo in caso di gravi guasti o straordinarie manutenzioni, e la loro coerenza in ogni momento.

4. Collegamento in modo sicuro con tutte le strutture.

Il collegamento per lo scambio dei dati avverrà per mezzo della già presente rete e il sistema dovrà garantirne la sicurezza e l'affidabilità nelle trasmissioni, tanto più quando i dati

scambiati saranno di tipo sensibile. Dovrà quindi mettere a disposizione un sistema di trasmissioni criptate.

5. Fornire uno strumento rapido ed efficace per la gestione delle password.
6. Dar la possibilità di gestire in modo completo ogni account.

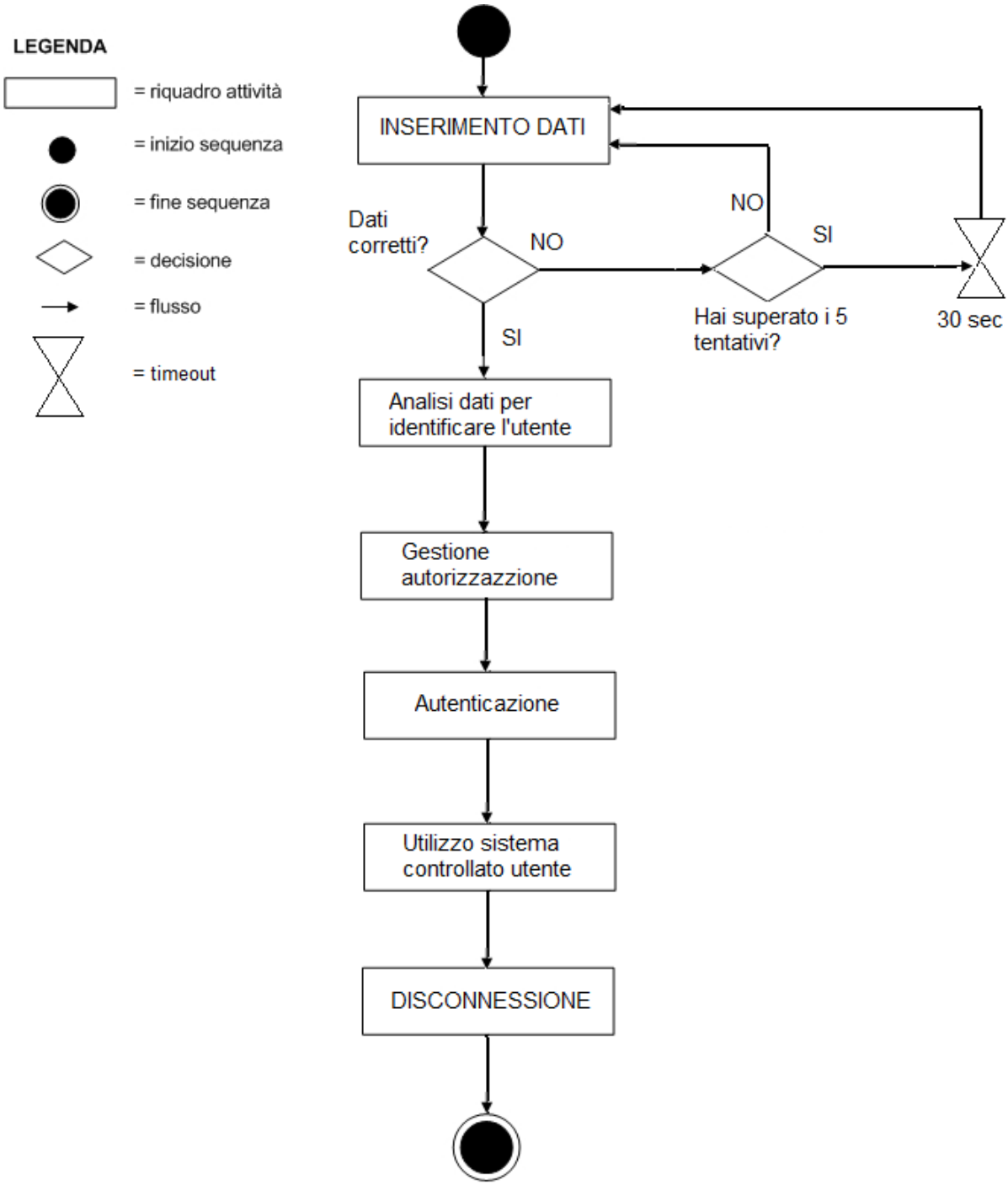
Gestire le autorizzazioni di ogni account durante tutto il suo ciclo di vita con la possibilità di poter bloccare e in seguito eliminare un account non più valido o attivo.

FATTORI CRITICI INDIVIDUALI

1. Semplicità di utilizzo del sistema. Gli utenti del sistema devono poter essere in grado di utilizzarne in maniera semplice ed immediata tutte le sue funzionalità
2. Semplicità di autenticazione attraverso il meccanismo di Sigle sign-on.

4.2.2. Descrizione delle esigenze funzionali

Lo scopo del progetto è la realizzazione di un sistema che permetta la facile gestione dei dati di ogni utente attraverso l'autenticazione con account creati per ogni singolo individuo presente all'interno delle strutture, il quale possiederà a seconda del proprio ruolo un diverso livello di autorizzazione. I dati comprenderanno oltre a quelli sensibili tutte le informazioni utili all'amministrazione (buste paga, giorni di ferie, ore di lavoro, periodi di malattia) necessari per la semplificazione delle procedure burocratiche quali ad esempio anche la timbratura del cartellino.
Si richiede inoltre al progetto di realizzare un software in grado di adempire agli obblighi normativi previsti dal codice in materia di privacy (D. Lgs. 196/03), garantire inoltre la disponibilità e integrità dei dati e delle applicazioni necessarie allo svolgimento dei processi e dei servizi forniti. Quando un utente registrato chiede l'accesso al sistema e ai vari dati in esso contenuti il software dovrà essere in grado di verificare le autorizzazioni di quel determinato utente e consentirne l'accesso o il rifiuto. L'utente potrà eventualmente richiede un'approvazione da parte di una persona autorizzata che a seconda del tipo di informazione alla quale vuole aver accesso rifiuterà o accetterà la richiesta.
Utilizziamo qui di seguito uno schema di tipo UML semplificato, illustrativo allo scopo di rendere più chiaro il processo di autenticazione.



Descrizione della modalità con cui avviene una richiesta di autenticazione

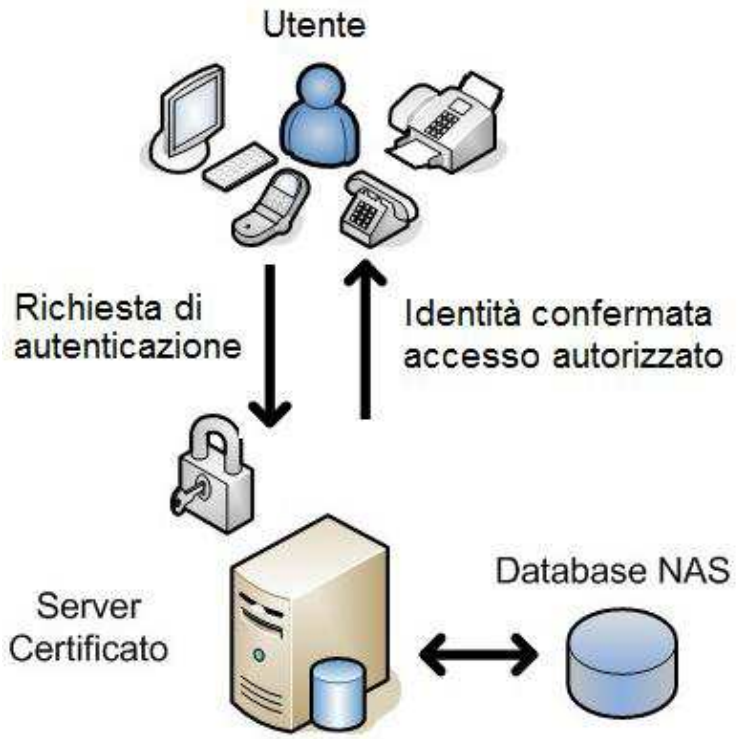
4.2.3. Descrizione delle esigenze dei dati

Il sistema deve tenere traccia di tutte le richieste pervenute, mantenendone uno storico.

Le informazioni che devono essere rilevate sono:

- Identificatore univoco di ciascun utente
- Dati personali quali nome, cognome, data nascita, luogo nascita, residenza, recapito telefonico, codice fiscale, ragione sociale
- Data e ora di registrazione
- Stato di impiego
- Ruolo ricoperto all'interno delle strutture.

I dati possono essere inseriti dall'utente stesso o da chi per lui ne possiede la facoltà come un amministratore di sistema che al momento dell'assunzione del dipendente o della registrazione dell'identità di un individuo, assume i dati che questo ha inserito in un modulo prestampato su carta e andrà ad inserire i dati all'interno del database o ad esempio in una pagina web attraverso form apposito per l'inserimento dei dati. A seconda del ruolo ricoperto l'utente avrà diversi livelli di autorizzazione nell'uso delle risorse del sistema. L'utente ha però la possibilità di inserire lui stesso i dati con l'aiuto di appositi form. I dati di registrazione e le informazioni sulle autorizzazioni devono prevedere una procedura di recupero in caso di guasto hardware.



Schema che rappresenta il flusso dei dati quando si accede al sistema di Identity Management

4.3. SITUAZIONE DI PARTENZA

4.3.1. Contesto organizzativo e processi

Attualmente all'interno delle strutture comunali non sono presenti sistemi atti all'identificazione dell'identità dell'utente che sfruttino le potenzialità della tecnologia attualmente presente nel mercato.
Il sistema presente consiste nell'archiviazione su vari database delle informazioni di ciascun dipendente ed utente generico. Ad ogni nuovo dipendente viene fornito al momento della assunzione una username ed una password attraverso le quali potranno accedere alle funzionalità abbastanza limitate del sistema in uso .
Questa coppia di valori viene usata soltanto come metodo per poter utilizzare le risorse informatiche, senza però avere un effettivo controllo sugli accessi e "chi accede" a "cosa accede".
Non è raro in questi sistemi che un utente dimentichi o smarrisca i documenti contenenti le informazioni riguardanti le chiavi di accesso, per queste o altre casistiche è presente un help desk formato da 4 persone che forniscono anche la loro assistenza e ricordano o modificano la password dell'utente sbadato.
L'ente vede varie strutture comunali collegate tra di loro attraverso rete pubblica e/o privata, che facilita la comunicazione e lo scambio di informazioni.
Non sono presenti all'interno dell'ente risorse per le quali sia possibile pensare di effettuare uno sviluppo in-house del software.

4.3.2. Tecnologia utilizzata

Le strutture d'interesse sono suddivise in 9 sedi dislocate in tutto il territorio comunale, queste comunicano tra di loro attraverso una rete privata INTRANET che ha come centro stella virtuale la sede del comunale di Cavarzere nel quale sono collocati tutti i principali sistemi di elaborazione e i dati.
La rete di comunicazione tra queste sedi è in parte complessa, si suddivide in una rete pubblica attraverso la quale comunicano tutte le sedi sedi, ed una rete privata attraverso le quali comunicano la sede comunale con la biblioteca ed un centro per il disaster recovery.
Importante sottolineare che le sedi che sono collegate sia alla rete pubblica che a quella privata hanno all'ingresso della rete pubblica un firewall che protegge l'accesso non autorizzato a quella privata.

L'insieme delle strutture hanno complessivamente in tutte le loro sedi 197 personal computer dei quali:
- 51 di recente aggiornamento con SO Windows Vista
- 103 con SO Windows Xp Professional Edition
- 43 con SO Windows 98

4.3.3. Dati esistenti

Attualmente i dati presenti all'interno delle strutture comunali riguardanti le informazioni personali di ciascun utente sono contenute in archivi database separati a secondo della tipologia dei dati stessi.
I dati vengono raccolti attraverso dei moduli che ciascun utente deve compilare al momento della sua assunzione e nei quali è richiesta l'approvazione per il trattamento dei dati personali ai fini di non infrangere la legge sulla privacy.

4.3.4. Analisi del mercato

Procediamo quindi con l'analisi delle soluzioni offerte dal mercato nelle varie tipologie.
Di seguito sono riportate alcune delle soluzioni in modalità di pacchetto applicativo, FOSS, realizzazione In-house e su commessa esterna elencandone le compatibilità dei vari software con le varie piattaforme, per una iniziale valutazione della soluzione migliore per il nostro cliente..

Soluzione pacchetto applicativo

Nome del prodotto: **Novell Identity Manager**
Fornitore: **Novell**

Componenti:

- *Hardware*
  Soluzione modulare costituita da:
  - Application Server
  - Web Server
  - Interface Server (Protocollo TCP /IP)
  - Applicativi di sicurezza
- *Software di base*
  - Novell Open Enterprise Server (OES) con il Service Pack più recente
  - NetWare 6.5 con il Support Pack più recente

- Windows 2000 Server con il Service Pack più recente (32 bit)
- Windows Server 2003 R2 con il Service Pack più recente (2003 a 64 bit non supportato)
- Windows XP Professional (solo Mobile iManager)
- Red Hat Linux AS 3.0 (Glibc versione 2.1.1 o successive e kernel versione 2.2.xx o successive)
- Red Hat Linux AS 4.0 per AMD 64/EM64T (solo iManager 2.6 SP1)
- Red Hat Linux 8 - 9 (solo iManager 2.5 FP3)
- Solaris 9 - 10 (solo iManager 2.6 SP1)
- SUSE Linux Enterprise Server 8, 9 o 10 con il Service Pack più recente

▪ *Software d'ambiente*
- MySQL 4.1.12 (incluso nel prodotto e impostazione predefinita)
- JBoss Application Server ver. 4.0.2
- Oracle o 9*i* (9.2.0.4)
- Oracle 10*g* (10.2.0.1.0)
- Microsoft SQL 2000 SP4

▪ *Software applicativo*
- Applicazione Client / Server Tradizionale Interfacciata a database SQL.
- Applicazione Web Oriented.

▪ *Ulteriori componenti tecnologiche*
- Dispositivi per il riconoscimento dell'utente quali : badge, lettore di schede, lettore biometrico o riconoscitore vocale

Novell Identity Manager come gli altri applicativi unifica le identità digitali di tutti i sistemi, affinché quando nel sistema autoritativo viene creata o modificata un'identità, le nuove informazioni vengano automaticamente propagate a tutti i sistemi interessati. Questo approccio consente di mantenere la conformità alle norme imposte.

Nome del prodotto: **OpenSSO Entrerprise 8.0**
Fornitore: **SunMicrosystems, Inc**.

Componenti

▪ *Hardware:*
- Minimo 1 Gb di RAM, consigliato 4Gb
- Spazio su disco: Server: 512MB per l'applicazione
- 7GB per i file di Log

- Client: 100MB per client SDK
- 5GB per file di log

- *Software di base:*
  - Solaris 9 -10 OS on SPARC, x86, and x64 based systems
  - OpenSolaris RedHat Enterprise Linux 5
  - RedHat Enterprise Linux 4 server (Base and
  - Advanced Platform, 64–bit onAMDservers)
  - Ubuntu 8.0.4
  - Windows Server 2003
  - Windows XP
  - Windows Vista
  - Windows 2008 Server
- *Software d'ambiente:*
  - *Server:* JDK 1.5.x or 1.6.x 64-bit JVM on supported web containers
  - *Client:* JDK 1.4.x, 1.5.x. or JDK 1.6.x
  - MySQL MySQL version 4.1.1
  - Oracle OracleDatabase 10g or later
- *Ulteriori Funzionalità:*
  Un ingegnere può inviare un URL interno per una specifica documentazione ad un'altro ingegnere che lavora per un'azienda partner.
  Un venditore può presentare una fattura al servizio contabile.

Nome del prodotto : **Oracle Identity Managment**
Fornitore: **Oracle**

Componenti

- *Hardware*
  soluzione modulare costituita da:
  - Application Server
  - User Web Server
  - Interface Server (Protocollo TCP /IP)
  - Applicativi di sicurezza

- *Software di base*
  come sistema operativo si può scegliere tra:
  - AIX 5L Version 5.3 (pSeries 64-bit)

- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2003 R2 (EMT/AMD/IA 64-bit)
- Oracle Enterprise Linux Release 4 , 5 (EMT/AMD 64-bit)
- Oracle Virtualization Server - EL4
- Red Hat Enterprise Linux AS Release 4 (EMT/ADM/IA 64-bit)
- Solaris Operating System 10 (UltraSparc 64-bit)
- HP-UX 11.23 (PA-RISC/IA 64-bit)
- SUSE Linux Enterprise Server 10 (EMT/AMD/IA 64-Bit)

▪ *Software d'ambiente*
si può scegliere tra:
- Oracle Database Deployment
- Oracle9*i* Database Enterprise Edition release 9.2.0.7 and later patch
- Oracle Database 10*g* , 11*g* Enterprise Edition releases
- Oracle RAC Deployment
- Oracle Database 10*g*, 11*g* Enterprise Edition release

▪ *Software appiicativo*
- BEA WebLogic Server 8.1 SP6 and later service packs
- IBM WebSphere Application Server 6.1.0.9 and later fix packs
- JBoss Application Server 4.0.3 SP1 and later service packs
- Oracle Application Server 10.1.3.3 (Upgrade patch 10.1.3.3 applied)

Per ogni clint SDK e Server application è necessaria la relase JDK 1.5.0 and later.

Nome del prodotto : **IBM Tivoli Identity Manager**
Fornitore: **IBM**

Componenti:

▪ *Hardware*
soluzione modulare costituita da:
- Database server
- Directory server
- Application server
- Messaging support
- Web server

Specifiche Hardware

Memoria di Sistema (RAM) 4 GB
Velocità processore Single 2.0 Ghz Intel o pSeries Dual 3.2 Ghz
Spazio su disco per il prodotto 25 GB

- *Software di base*
  Come sistema operativo si può scegliere tra:
  - AIX 5.3 Solaris 10
  - Windows Server 2003
  - Red Hat Linux 4.0 and 5.0
  - SUSE Linux 9.0 and 10.0
  - HP-UX 11i v2, 3 (PA-RISC, Itanium)

- *Software di ambiente*
  - IBM DB2® Enterprise Version 9.1
  - Microsoft SQL Server 2005, Enterprise Edition
  - Oracle 10g Release 2 (Version 10.2.0.1)

- *Software applicativo*
  - WebSphere Application Server, Version 6.1

Realizzazione in-house

Per la realizzazione in house non sono disponibili le risorse interne necessarie allo sviluppo.

Commessa esterna

Questa modalità di realizzazione prevede la creazione ex novo del software e di tutte le sue componenti da parte di un'azienda esterna specializzata nello sviluppo di software. Presuppone quindi una lunga analisi della soluzione migliore da adottare, un periodo di collaudo più lungo rispetto alla soluzione a pacchetto applicativo perché il software è di nuova creazione e l'adattamento dell'hardware presente con i nuovi componenti del nuovo software.

4.3.5. Vincoli

- ✓ *Normativi*

In relazione alla normativa sulla privacy, è necessario fare firmare un documento agli utenti con il quale viene consentito dall'utente il trattamento dei dati personali anche se in forma strettamente confidenziale e protetta ai soli fini burocratici.
Persone non autorizzate non possono avere accesso a tali informazioni.

- ✓ *Economici*

Il tetto di spesa assegnato alla realizzazione del sistema è pari a 50000,00 €.

- ✓ *Organizzativi*

Il numero massimo di tecnici informatici che devono seguire il sistema durante il suo funzionamento è di tre addetti.

- ✓ *Temporali*

Il tempo a disposizione per lo sviluppo e l'avviamento del sistema non deve superare i 18 mesi.

- ✓ *Tecnologici*

Compatibilità con DBMS MySQL e Oracle (se previsto l'utilizzo di un DBMS).

- ✓ *Raccomandazioni*

La soluzione più comoda ed efficace per l'autenticazione degli utenti al sistema consisterebbe nell'utilizzo di dati biometrici.
Data però la sensibilità di tali dati, il loro utilizzo è stato sconsigliato da parte dei committenti.
Si consiglia lo sviluppo di un sistema di facile utilizzo e il più automatizzato possibile.

4.4. IPOTESI DI LAVORO

4.4.1 Considerazioni

4.4.1.1 Considerazioni sulle esigenze rilevate

Si ritiene indispensabile mantenere la spesa all'interno del tetto massimo che è stato definito dal committente, inoltre è preferibile scegliere soluzioni che si integrino il più possibile con i dati, l'hardware e la tecnologia già esistente in modo tale da ridurne l'impatto organizzativo e di conseguenza la spesa finale.
Il sistema da realizzare dovrà essere di semplice utilizzo anche per utenti inesperti e quindi non dovrà richiedere particolari conoscenze perché tutte le sue potenzialità vengano utilizzate.
Tale sistema dovrà fornire delle semplici funzionalità che gestiscano il riconoscimento delle utenze comunali e ne fornisca le autorizzazioni per l'utilizzo di tale sistema.
Andrà installato presso tutte le strutture comunali in modo tale da garantire l'accessibilità e la disponibilità a tutti gli utenti.
L'utilizzo sarà permesso ai soli membri registrati tramite l'inserimento di dati personali di controllo attraverso i quali l'utente verrà identificato.
I dati di identificazione potranno essere di tipo biometrico, con l'uso di tessera magnetica o semplicemente consistente di username e password. Fattore fondamentale è la possibilità di gestire l'account dell'utente per l'intero ciclo di vita all'interno nel suo ambito di interesse con possibilità di modificarlo, bloccarlo o eliminarlo in qualsiasi momento, ad esempio quando un dipendente viene licenziato.
Andranno verificate le autorizzazioni dell'utente e a seconda del ruolo ricoperto all'interno delle strutture sarà consentito l'accesso e l'utilizzo di applicazioni, dati e servizi. Dovranno essere previste delle procedure per garantire la disponibilità dei dati, delle applicazioni e dei servizi necessari allo svolgimento dei processi.

4.4.1.2 Considerazioni sulla situazione interna

La realizzazione di tale sistema non modifica i processi comunali, ma ne permette una più veloce esecuzione grazie all'automatizzazione delle varie procedure. Il sistema si servirà della già presente struttura di comunicazione già sufficiente a supportare il nuovo sistema e utilizzerà in gran parte l'hardware già presente con gli eventuali adattamenti necessari per adempire alle varie compatibilità software. Sarà invece necessario introdurre un nuovo Server che gestisca tale software e che si appoggi sullo stesso tipo di database già esistente per rendere meno onerosa la migrazione dei dati. Infine il sistema prevederà l'uso di client già esistenti, ai quali sarà installato il software necessario per permettere agli utenti di

identificarsi con i mezzi che gli sono stati forniti al momento della sua registrazione e che gli daranno l'accesso ai servizi e ai dati in base al ruolo che ricopre.

Naturalmente l'introduzione di questo nuovo sistema dovrà prevedere un periodo di formazione di tutte quelle persone che ne faranno uso, specialmente per quanto riguarda i tecnici informatici che dovranno amministrare il software.
Per ridurre al minimo questo periodo il software dovrà essere di semplice utilizzo e di facile accesso con procedure automatizzate di registrazione e gestione delle password in caso di perdita.

4.4.1.3 Considerazioni sul mercato

Analizzando le offerte disponibili sul mercato ci si rende conto come sia disponibile una grande offerta per ciò che concerne il tipo di software che andiamo a ricercare sotto forma di pacchetto applicativo. Verrà comunque considerata una soluzione su commessa esterna per confrontarne le differenze con le altre soluzioni.

Soluzione FOSS

Il prodotto proposto dall'azienda Sun Microsystems Inc. è sicuramente un prodotto completo e presenta molte funzionalità aggiuntive che possono in ogni momento divenir utili. Il punto di forza di questa soluzione è sicuramente il fatto che sia un prodotto Open Source quindi dal costo praticamente nullo, ma purtroppo senza un sicuro supporto in caso di problemi al software se non quello offerto da una pur sempre grande comunità.

Soluzioni pacchetto applicativo

Un prodotto molto completo è offerto da Oracle, senza dubbio una tra le più grandi società in ambito di software aziendale e database. Questo software permette di gestire l'intero ciclo di vita delle identità degli utenti su tutte le risorse comunali, sia all'interno che all'esterno del firewall. In particolare, permette di implementare le applicazioni con maggiore rapidità, applicare una protezione più dettagliata alle risorse comunali, eliminare automaticamente i privilegi di accesso latenti e molto altro ancora. Tale offerta seppur presenti un prodotto di elevato livello molto completo, offrendo supporto e servizio on-site assicurato, ha il difetto di aver un costo troppo elevato per il budget che è stato riservato.

Altra soluzione la offre Novell. Assicura infatti un software con un'elevata scalabilità adattabile ad ogni evenienza, con semplicità d'uso e di reset delle password. Conforme e dinamico, registra tutti gli accessi e ne offre a chi ne ha il potere di controllarli.

Infine altro prodotto di un'azienda da sempre all'avanguardia nel settore software è quello proposto dalla IBM. IBM Tivoli Identity Manager interagisce direttamente con gli utenti e con due tipi di sistemi esterni: i meccanismi di controllo accessi e le origini di identità. Questi sistemi forniscono informazioni affidabili sugli utenti che necessitano degli account. Ma allo stesso tempo integrano tutte le funzioni più avanzate che fanno parte di un sistema di Identity Management di alto livello.

Soluzione commessa esterna

La soluzione su commessa esterna non è stata specificata, ma sarà analizzata dettagliatamente in seguito nell'analisi del rischio. Si ribadisce come questo tipo di soluzione preveda tempi lunghi per la realizzazione del software del collaudo e formazione degli utenti per un software completamente nuovo.

4.4.1.4 Considerazioni sui vincoli

Esistono dei *vincoli normativi* che impediscono la completa informatizzazione del sistema.
I software presi in esame manipolano informazioni personali che sono soggette alla legge sulla privacy nonché al d.lgs. 196/03 le cui finalità consistono nel riconoscimento del diritto del singolo sui propri *dati personali* e, conseguentemente, nella disciplina delle diverse operazioni di gestione dei dati, riguardanti la raccolta, l'elaborazione, il raffronto, la cancellazione, la modificazione, la comunicazione o la diffusione degli stessi. Il diritto sui propri dati è differente dal *diritto alla riservatezza*, in quanto non riguarda solamente informazioni inerenti la propria vita privata, ma si estende in generale a qualunque informazione relativa ad una persona, anche se non coperta da riserbo (sono dati personali ad esempio il nome o l'indirizzo della propria abitazione).
Lo scopo della legge non è quello di impedire il trattamento dei dati, ma di evitare che questo avvenga contro la volontà dell'*avente diritto*, ovvero secondo modalità pregiudizievoli. Infatti il testo unico definisce i diritti degli interessati, la modalità di raccolta e i requisiti dei dati, gli obblighi di chi raccoglie, detiene o tratta dati personali e le responsabilità e sanzioni in caso di danni. E' necessario quindi utilizzare documenti cartacei che possano essere firmati dal nuovo utente e che ne permetta il trattamento dei dati personali nel momento della registrazione e dell'uso di tali informazioni sul sistema.

Le soluzioni in modalità di pacchetto applicativo offrono già una sicura conformità per quanto riguarda i vincoli di tipo normativo in quanto sono software che sono già presenti su più realtà aziendali e pienamente collaudati. La compatibilità delle varie proposte con la tecnologia esistente è garantita e i tempi di consegna e di formazione del personale rispetta i termini massimi imposti. Grazie all'elevato sistema di automatizzazione sarà ora possibile la riduzione del personale addetto alla gestione del sistema con una conseguente riduzione delle spese di gestione. Per tutte le soluzioni i tempi massimi di consegna sono rispettati anche se nella soluzione su commessa esterna abbiamo un ridotto margine che offre poca sicurezza nel caso si dovessero incontrare problematiche nello sviluppo del software.

Per quanto riguarda invece i vincoli di tipo economico notiamo come la soluzione proposta da Oracle non sia attuabile perché il costo totale è troppo elevato e supera il budget massimo imposto, anche se il programma è molto completo e fornito di molti componenti aggiuntivi che possono venir utili qualora si volesse ampliare il proprio sistema di Identity Management a più applicazioni esterne.

4.4.2. Ipotesi di soluzione

Obiettivi:

- Unificare le identità digitali di tutti i sistemi, affinché quando nel sistema autoritativo viene creata o modificata un'identità, le nuove informazioni vengano automaticamente propagate a tutti i sistemi interessati.
- Creare un'area di autorizzazioni basate sui ruoli, che consente di definire e gestire le autorizzazioni basandosi sui ruoli; fare in modo che le nuove utenze abbiano accesso a tutto ciò di cui hanno bisogno per iniziare subito a lavorare.
- Gestire l'account in modo completo per l'intero ciclo di vita con possibilità di bloccarlo o/e eliminarlo
- Dimostrare, controllare, automatizzare e verificare le norme di sicurezza controllando in tempo reale le eventuali violazioni della sicurezza e dimostrando che soltanto gli utenti autorizzati hanno accesso a informazioni e sistemi riservati

Componenti della soluzione:

In tutte le ipotesi di soluzione si considera la stessa base hardware, software di base e di ambiente. Nel dettaglio:

Componenti comuni alle soluzioni:

1. NAS WD ShareSpace WDA4NC40000
2. Server IBM System x3200 M2
3. Lettori di badge, almeno uno per ogni reparto
4. Utilizzo software di base Windows server 2003 già presente
5. Acquisizione licenza software di base Windows XP Professional Edition per i client con software con tecnologia inferiore
6. Utilizzo software d'ambiente Oracle 10g Release 2 già presente

La scelta del software si differenzia nelle seguenti ipotesi di soluzione:

A. Pacchetto applicativo Novell Identity Manager

Novell Identity Manager come gli altri applicativi unifica le identità digitali di tutti i sistemi societari, affinché quando nel sistema autoritativo viene creata o modificata un'identità, le nuove informazioni vengano automaticamente propagate a tutti i sistemi interessati., ha la possibilità di interfacciarsi con il supporto RDBMS Oracle, di cui si possiedono già le licenze. Necessita quindi di un server applicativo compatibile con il DBMS Oracle, ma può funzionare anche con sistemi Open Source quali MySQL o PostgreSQL.
L'applicativo poi è compatibile con numerosi software di base tra cui Windows Server 2003 il più diffuso all'interno dei server aziendali e del quale si dispone già della licenza.

B. Pacchetto applicativo OpenSSO Enterprise 8.0 di Sun Microsystems, Inc.

Versione Open Source di Sun che nonostante sia appunto una soluzione non a pagamento è compatibile con molte soluzioni all'interno del mercato, ha anch'essa infatti la compatibilità con il software per server di base Microsoft ossia Windows server 2003 ed è inoltre compatibile con Oracle oltre che a MySQL. Offre un buon livello di personalizzazione e la possibilità di disporre del codice sorgente qualora si disponga di uno staff competente per la modifica del software.

C. Pacchetto applicativo IBM Tivoli Identity Manager

Soluzione completa sviluppata da IBM garantisce anch'essa compatibilità con i maggiori software di base e di ambiente. Fornisce una soluzione sicura e automatica di gestione delle utenze basata su criteri che consente di gestire in modo efficiente account utente, password e autorizzazioni di accesso in ambienti IT. Questa soluzione automatizza i processi di creazione, provisioning o de-provisioning dei privilegi utenze di risorse IT eterogenee per l'intero ciclo di vita dell'utente. Fornisce inoltre un avanzato sistema di reset e di gestione delle password personali da parte dell'utente.

D. Realizzazione su commessa esterna

In questo caso la valutazione è complicata in quanto dipende dall'azienda alla quale sarà affidata la realizzazione del software, comunque è preferibile cercare di ottenere un software il più possibile adattato alla realtà tecnologica presente nelle strutture di nostro interesse per ridurre il più possibile le spese e i tempi per l'aggiornamento hardware e software.

Fasi di realizzazione

Le fasi di realizzazione per quanto riguarda i pacchetti applicativi sono comuni a tutte e 3 le soluzioni valutate quindi vengono presentate insieme.

Soluzione 'pacchetto applicativo' A, B, C:
A) Acquisto del prodotto e personalizzazione;
B) Installazione;
C) Migrazione dati;
D) Formazione utenti;
E) Periodo di prova.

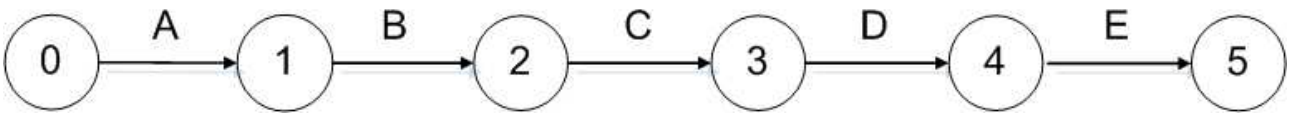


Figura A

Soluzione D:

A) Redazione bando e concorso pubblico;
B) Riunioni ed eventuali proposte aziende;
C) Tempo realizzazione software;
D) Formazione utenti;
E) Alpha Test e Beta Test;
F) Rilascio e installazione.

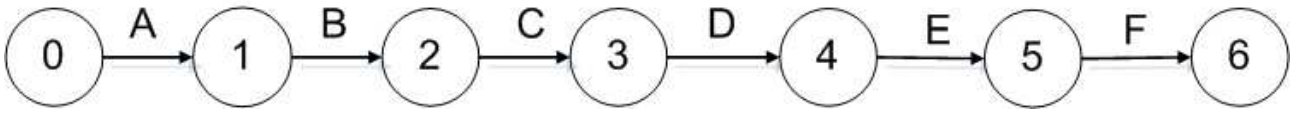


Figura B

Fig. A fig. B sono l grafi CPM che mostrano la sequenza temporale delle attività da svolgere per completare il progetto e l'avviamento del sistema.

Tempificazione orientativa

Soluzione 'pacchetto applicativo' A, B, C:

- Tempo di acquisto, personalizzazione e installazione è di 90 giorni lavorativi;
- Tempo migrazione dati è di 90 giorni lavorativi;
- La formazione degli utenti è prevista in tre lezioni (3 giorni lavorativi);
- La formazione dei tecnici informatici è prevista di due corsi giornalieri (2 giorni lavorativi)
- Periodo di prova e avvio del sistema necessario è di 180 giorni lavorativi.

Tot. 365 giorni lavorativi.

Soluzione D:

- Dall'inizio del progetto passano 30 giorni per ottenere risposte al bando valide dalle aziende e valutare le migliori;
- Tempo di realizzazione del software previsto 240 giorni lavorativi;
- La formazione degli utenti è prevista in tre lezioni (6 giorni lavorativi);
- Per l'installazione e i test (Alpha e Beta) si prevede un periodo di 120 giorni lavorativi;
- Avvio e prova richiederanno un tempo di 30 giorni lavorativi.

Tot. 426 giorni lavorativi.

Benefici attesi

Per tutte le soluzioni si prospettano i seguenti benefici:

- Centralizzare la definizione di utenti e il provisioning dei servizi utente per ridurre le complessità di gestione da più interfacce native
- Ridurre gli errori causati dai processi di business manuali automatizzando le richieste di approvazione e di invio degli utenti
- Fornire funzioni di riconciliazione e un toolkit di gestione delle applicazioni per integrare i cambiamenti, come fusioni e acquisizioni
- Supportare l'instradamento dinamico delle approvazioni per automatizzare i processi di inoltro e approvazione per le richieste di accesso e cambiamento delle informazioni utente
- Includere meccanismi di auditing e reporting per consentire agli amministratori di produrre report che specificano chi può accedere a quali risorse
- Fare in modo che le nuove utenze abbiano accesso a tutto ciò di cui hanno bisogno per iniziare subito a lavorare
- Continuare a utilizzare le applicazioni di cui si disponeva, ma renderle più sicure
- Liberare l'help desk da tutte le attività correlate alla modifica delle password degli utenti, ossia fare in modo che gli utenti possano modificare le password e gestire le loro identità nel rispetto delle norme.
- Diminuzione dei costi delI' IT
- UNA PERSONA UN'IDENTITA'

4.4.3. Analisi del rischio

A. Pacchetto applicativo Novell Identity Manager

Fattore di rischio	Peso	Descrizione
Dimensione del progetto	Basso	Tempi ridotti, basso rischio dovuto alla conoscenza del pacchetto applicativo. L'unico problema deriva dalla personalizzazione.
Esperienza nella problematica	Basso	Ci si affida ad un team con esperienza nel settore
Esperienza nella tecnologia	Medio	
Livello di strutturazione	Medio	
Impatto organizzativo	Alto	Comporta un sostanziale cambiamento delle metodologie di utilizzo dei servizi e delle applicazioni
Capacità organizzativa	Medio	

Tabella relativa all'analisi del rischio del pacchetto applicativo Novell Identity Manager

B. Pacchetto applicativo OpenSSO Enterprise 8.0

Fattore di rischio	Peso	Descrizione
Dimensione del progetto	Basso	Tempi ridotti, basso rischio dovuto alla conoscenza del pacchetto applicativo. L'unico problema deriva dalla personalizzazione.
Esperienza nella problematica	Basso	Ci si affida ad un team con esperienza nel settore
Esperienza nella tecnologia	Basso	
Livello di strutturazione	Medio	
Impatto organizzativo	Alto	Comporta un sostanziale cambiamento delle metodologie di utilizzo dei servizi e delle applicazioni
Capacità organizzativa	Medio	

Tabella relativa all'analisi del rischio del pacchetto applicativo OpenSSO Enterprise 8.0

C. Pacchetto applicativo IBM Tivoli Identity Manager

Fattore di rischio	Peso	Descrizione
Dimensione del progetto	Basso	Tempi ridotti, basso rischio dovuto alla conoscenza del pacchetto applicativo. L'unico problema deriva dalla personalizzazione.
Esperienza nella problematica	Basso	Ci si affida ad un team con esperienza nel settore
Esperienza nella tecnologia	Basso	
Livello di strutturazione	Medio	
Impatto organizzativo	Alto	Comporta un sostanziale cambiamento delle metodologie di utilizzo dei servizi e delle applicazioni
Capacità organizzativa	Basso	Sistema semplice con molte funzionalità

Tabella relativa all'analisi del rischio del pacchetto applicativo IBM Tivloli Identity Manager

D. **Realizzazione su commessa esterna**

Fattore di rischio	Peso	Descrizione
Dimensione del progetto	Alto	Alta probabilità di errore nel rispettare i requisiti durante lo sviluppo dell'applicativo. Tempi necessariamente più lunghi.
Esperienza nella problematica	Basso	Ci si affida ad un team con esperienza nel settore
Esperienza nella tecnologia	Medio	Bisogna acquisire la conoscenza del software sviluppato.
Livello di strutturazione	Medio	
Impatto organizzativo	Alto	Comporta un radicale cambiamento delle metodologie di utilizzo dei servizi e delle applicazioni
Capacità organizzativa	Medio	

Tabella relativa all'analisi del rischio della realizzazione su commessa esterna del sw

4.4.4. Soluzione/i da valutare

Analizzando le soluzioni proposte possiamo da subito notare come la soluzione su commessa esterna presenta un rischio troppo elevato per l'ente dato soprattutto dalla creazione da zero di un nuovo programma che necessita di un lungo periodo di sviluppo, collaudo, avvio del software e per la formazione non solo degli utenti ma anche dei tecnici interni addetti alla gestione del sistema informativo. Inoltre dato la vasta proposta sul mercato di pacchetti applicativi già pronti e testati non è una buona scelta quella su commessa esterna, che avrebbe necessariamente costi maggiori, anche se il software sarebbe creato su misura. Sebbene i pacchetti software necessitino di una personalizzazione, si presentano comunque come software già pienamente testati, molto completi e ben flessibili che si adattano bene alle varie esigenze che possono insorgere all'interno delle strutture comunali. La nostra scelta sarà quindi orientata verso il pacchetto applicativo. Tra le varie opzioni troviamo anche la soluzione Open Source offerta dalla Sun, grande azienda produttrice di software di elevata qualità, che in parte troviamo oramai in quasi tutti i nostri computer (Suite Java). Tuttavia questa soluzione non offre supporto adeguato per un'ente come il nostro cliente, se non quello che può essere garantito da una grande comunità che ci lavora per migliorarlo sempre, sebbene il software sia già testato e funzionante in varie realtà lavorative. Ci si trova quindi a dover scegliere fra le soluzioni di Novell e IBM. La nostra scelta, dopo aver effettuato un confronto delle varie caratteristiche e dell'analisi del rischio cade su IBM, ritenendo l'azienda una delle migliori in questo campo con un software assolutamente completo e all'avanguardia nel settore. Essendo quindi la scelta di IBM l'unica realmente realizzabile e sicura procediamo con l'analisi nel dettaglio di questa soluzione.

4.5. PROGETTO DI MASSIMA

4.5.1. Obiettivi

- Fare in modo che le nuove utenze abbiano accesso a tutto ciò di cui hanno bisogno per iniziare subito a lavorare
- Fornire ai dipendenti ciò di cui hanno bisogno a seconda del ruolo ricoperto
- Dimostrare, controllare, automatizzare e verificare le norme di sicurezza
- Liberare l'help desk da tutte le attività correlate alla gestione account
- Riduzione dei costi dell' IT

FARE IN MODO CHE LE NUOVE UTENZE ABBIANO ACCESSO A TUTTO CIÒ DI CUI HANNO BISOGNO PER INIZIARE SUBITO A LAVORARE

Ciò significa poter accelerare il processo di provisioning dei nuovi utenti riducendone i tempi ed eliminando le complesse e tediose procedure manuali associate solitamente alle nuove assunzioni ed utenze. Inoltre, tutte le operazioni sono verificabili, per consentire di applicare tutte le norme di sicurezza e di *dimostrarne* la conformità.
Eseguire il provisioning automatizzato per l'intero ciclo di vita degli utenti, garantendo l'accesso ai nuovi utenti sin dal primo giorno e modificando e bloccando l'accesso a tutti i sistemi quando necessario. Il sistema deve consentire di controllare i costi di amministrazione degli utenti, eliminare le procedure manuali complesse e applicare norme di sicurezza imposte dalla pubblica amministrazione, fornendo ai diversi utenti l'accesso alle risorse appropriate per svolgere il loro lavoro.

Automatizzare le procedure complesse di provisioning affinché gli utenti possano avere accesso immediato alle risorse di tutto il comune. Grazie al provisioning basato su ruoli, è possibile assegnare risorse agli utenti in base ai ruoli e alle norme della pa. I nuovi dipendenti hanno così la possibilità di accedere a tutte le risorse necessarie sin dal primo giorno di assunzione e in generale le nuove utenze possono da subito accedere ai contenuti a loro destinati, tutti i workflow di approvazione sono automatizzati. Semplificare, inoltre, la gestione degli accessi degli utenti, limitando il ricorso all'amministratore di rete centrale. Quando i ruoli cambiano, i diritti di accesso vengono aggiornati automaticamente. E quando un dipendente lascia il lavoro, il suo accesso viene revocato in tempo reale.

FORNIRE AI DIPENDENTI CIÒ DI CUI HANNO BISOGNO A SECONDA DEL RUOLO RICOPERTO

Nel corso della loro carriera professionale all'interno di un'organizzazione, i dipendenti possono ricoprire più di un ruolo. Il programma deve consentire di gestire automaticamente e in sicurezza le esigenze di accesso degli utenti, anche quando i ruoli cambiano e vengono assegnate nuove responsabilità, creare quindi un'area di autorizzazioni basate sui ruoli, che consente di definire e gestire le norme di autorizzazione basate sui ruoli. Queste norme assegnano autorizzazioni a gruppi specifici di utenti per appartenenze e conti in vari sistemi connessi.

DIMOSTRARE, CONTROLLARE, AUTOMATIZZARE E VERIFICARE LE NORME DI SICUREZZA

Registrare e tenere sotto controllo tutti gli accessi ai fini delle revisioni. Queste funzioni devono controllare in tempo reale le eventuali violazioni della sicurezza e dimostrare che soltanto gli utenti autorizzati hanno accesso a informazioni e sistemi riservati.
Gli ex-utenti rappresentano spesso un rischio, ma Identity Manager elimina questo problema cronico. Nel momento in cui lo stato del dipendente viene modificato in "licenziato" o utente non più attivo, nel database delle risorse umane o in qualsiasi altra fonte autoritativa, l'accesso alle risorse viene automaticamente revocato. Le risorse riservate rimangono così al sicuro.
Se, da una parte, solo le persone giuste devono poter accedere alle informazioni, dall'altra bisogna anche essere in grado di dimostrare che ciò avviene. Una soluzione per la gestione delle identità verificabili è un componente critico e deve essere incluso nelle funzionalità. Il sistema deve essere inoltre in grado di generare degli avvisi nel caso in cui vengano concessi accessi non adeguati.

LIBERARE L'HELP DESK DA TUTTE LE ATTIVITÀ CORRELATE ALLA GESTIONE ACCOUNT

Molte delle chiamate ricevute agli help desk da parte dagli utenti è correlato alle password. Rendere autonomi gli utenti eviterebbe problemi e distrazioni dal lavoro e aumenterebbe l'efficienza. E' possibile far in modo che gli utenti possano modificare le password e gestire le loro identità nel rispetto delle norme e liberare l'help desk da questo carico di lavoro. Solitamente un utente che dimentica la propria password deve chiamare l'help desk per richiederne il ripristino, perdendo tempo prezioso e aumentato i costi del supporto. Il sistema consente di sincronizzare le password degli utenti fornendo un'unica password per tutti i sistemi, che sarà più facile da ricordare. Si può inoltre fare in modo che le password impostate dagli utenti siano sicure, creando e applicando norme rigide per tutti i sistemi che proteggono le strutture da attacchi mirati alle password.

Quando un utente dimentica la propria password, entra in gioco l'applicazione utente, che consente di creare, modificare e ripristinare la password senza chiamare l'help desk e far perdere prezioso tempo.
Accedendo all'applicazione utente, quest'ultimi potranno utilizzare una delle opzioni seguenti in base all'impostazione dell'amministratore:

- *Suggerimenti* - L'amministratore stabilisce se il sistema deve fornire dei suggerimenti direttamente sullo schermo o via e-mail.
- *Ripristino mediante domanda e risposta* - Sullo schermo vengono visualizzate una o più domande. Questa opzione può includere domande originariamente create dall'utente, dall'amministratore di sistema o di entrambi i tipi. Quando l'utente risponde correttamente alle domande, può modificare la propria password. Il sistema verifica automaticamente la conformità della password alle norme, quindi aggiorna e sincronizza tutti i sistemi connessi.

RIDUZIONE DEI COSTI DELL' IT

La riduzione dei costi dell'IT è dovuta alla diminuzione del carico di lavoro dell'help desk il quale viene in parte automatizzato e gestito dall'utente stesso.

4.5.2. Funzioni del sistema

Tivoli Identity Manager assicura servizi e componenti delle seguenti aree:

- Controllo e gestione degli account
- Gestione attraverso Workflow dell'intero ciclo di vita degli account
- Politiche di provisioning
- Controllo degli accessi basati sui ruoli
- Autoregolamentazione dell'account utente
- Personalizzazione

CONTROLLO E GESTIONE DEGLI ACCOUNT

Con una soluzione efficiente di controllo degli accessi è possibile rintracciare precisamente chi ha avuto accesso ed a quali informazioni.
Il controllo degli account è una funzione critica di un sistema con un singolo punto dal quale vengono assegnati i ruoli, privilegi e risorse degli utenti.

Account orfani sono account attivi che non sono associati ad utenti validi, per questo tipo di account non è possibile risalire automaticamente dal sistema di provisioning al loro proprietario. Per risolvere questo problema vengono collegate insieme le informazioni di questi particolari account con quelle degli utenti che hanno account attivi, tipicamente mantenute all'interno di un database per rilevarne eventuali ridondanze.

Account configurati impropriamente sono account attivi che sono associati ad utenti validi ai quali sono state concesse impropriamente autorizzazioni perché gli amministratori del sistema possono aggiungere o modificare gli utenti al di fuori del sistema di Identity Manager. La capacità di controllare gli account impropri è molto più difficile e richiede un confronto di " cosa dovrebbe essere " con " che cos'è " al livello di autorizzazione account.
In un sistema IT complesso gli account comprendono centinaia di parametri e questi dettagli possono essere controllati dal sistema di provisioning.

Account nuovi possono essere facilmente identificati utilizzando i dati che vengono stabiliti dagli amministratori, una richiesta di accesso per la creazione di un nuovo utente avvia il processo che approva (o rifiuta) le risorse di cui è stato richiesto l'utilizzo.

GESTIONE ATTRAVERSO WORKFLOW DELL'INTERO CICLO DI VITA DEGLI ACCOUNT

Quando un nuovo utente viene creato, il ciclo utente ha inizio. Le politiche delle strutture di nostro interesse e i suoi processi, siano essi manuali o semi-automatizzati, abilitano l'utente all'accesso a certe risorse basate su ruoli e responsabilità. Nel tempo, quando il ruolo dell'utente e le sue funzioni cambiano, possono essere messe a disposizione nuove risorse che dovranno essere disponibili all'utente. Inoltre nell'eventualità che l'utente non faccia più parte delle strutture comunali, il suo account può essere sospeso e cancellato in seguito, terminando così il suo ciclo di vita. E' possibile utilizzare workflows per personalizzare le autorizzazioni degli account ed il loro intero ciclo di vita e come aggiungere rimuovere o modificare utenti ed account. Un completo sistema di provisioning basato su workflow guida automaticamente le richieste ai relativi approvatori e preventivamente le intensifica ad altri approvatori in caso in cui non vengano prese in esame.

Possono essere definiti due tipi di workflow nel sistema di Identity Manager. Wokflow dei diritti usati per le attività di definizione dei privilegi e dei ruoli, e workflow operazionali che si applicano ai tipi di entità. Un *wokflow dei diritti* definisce la logica del business che è legata specificatamente alle azioni di provisioning dalle politiche di provisioning. Una politica di provisioning dei diritti lega le azioni di provisionig con i workflow dei diritti. Per esempio un workflow dei diritti è usato per definire le approvazioni per la gestione degli account. Un

workflow operazionale invece definisce la logica del business per il ciclo di vita dei processi per i tipi di entità e le entità stesse. E' possibile utilizzare strumenti di programmazione per automatizzare aspetti chiave del ciclo di vita di provisioning, specificando i processi approvati che vengono usati. Un workflow di oggetti nella struttura comunale può contenere uno o più partecipanti e la loro graduatoria. Un partecipante consiste nella la firma di un'autorità che approva o rifiuta una richiesta di provisioning.

POLITICHE DI PROVISIONING

Ad una entità organizzativa basata su delle regole è assegnata una o più identità quando si implementa un controllo degli accessi basto su regole.
Le regole organizzative sono controllate da una *politica di provisioning* che rappresenta una serie di regole organizzative che forniscono la logica che il Server di sistema usa per gestire le risorse come applicazioni o sistemi operativi. Questa politica gestisce gli utenti in modo che ognuno abbia proprie regole e imposta i diritti di accesso che questi hanno quando tentano di accedere ad un servizio. La politica adottata deve riflettere anche il piano di sicurezza interno delle varie strutture comunali. Per implementarne una adatta è necessario prima analizzare i processi all'interno delle varie strutture e determinare quali miglioramenti possono essere fatti a questi processi per poter realizzare una soluzione di identity managment automatizzata.
Quando due o più politiche di provisioning vengono approvate, una direttiva di unione definisce come gestire gli attributi. Due o più politiche potrebbero avere degli scopi in comune e la direttiva di unione specifica che azione devono essere intraprese quando si verifica questo conflitto.

CONTROLLO DEGLI ACCESSI BASATI SUI RUOLI

Role-based access control (RBAC) utilizza la politica di provisioning e delle regole per valutare, testare e migliorare i processi e le regole che garantiscono l'accesso agli utenti.
Gli amministratori creano politiche di provisioning e assegnano agli utenti le regole che definiscono una serie di diritti di accesso alle risorse a seconda delle regole impostate.
RBAC stabilisce appunto il controllo degli accessi basati sui ruoli, questo valuta i cambiamenti alle informazioni dell'utente per determinare se i cambiamenti alterano anche le regole di accesso consentite a tale utente. Se è necessario un cambiamento, le politiche sono riviste e i cambiamenti dei diritti vengono effettuati immediatamente. Analogamente, un cambiamento nell'insieme di definizione delle regole in una politica può provocare un cambiamento agli utenti associati.
RBAC include ulteriori funzionalità quali:

- *Diritti obbligatori od opzionali:* quando vi sono diritti opzionali questi non sono automaticamente gestiti ma possono essere richiesti da un utente in un gruppo
- *Servizi prerequisiti:* quando servizi specifici devono essere garantiti prima che certe regole di accesso vengano impostate
- *Personalizzazione dei diritti:* dove ogni caratteristica di un diritto può essere impostata ad un valore di default od a un valore personalizzato a seconda dei permessi che vengono concessi da tale diritto
- *Segretezza:* le informazioni sugli utenti e le applicazioni vengono filtrate
- L'approccio di autenticazione dell'utente è conforme alle politiche interne di sicurezza
- *Sicurezza:* garantita anche con l'accesso alla rete WAN ed Internet includendo firewall incrociati
- Algoritmi per la definizione dello User ID definiti dall'utente

AUTOREGOLAMENTAZIONE DELL'ACCOUNT UTENTE

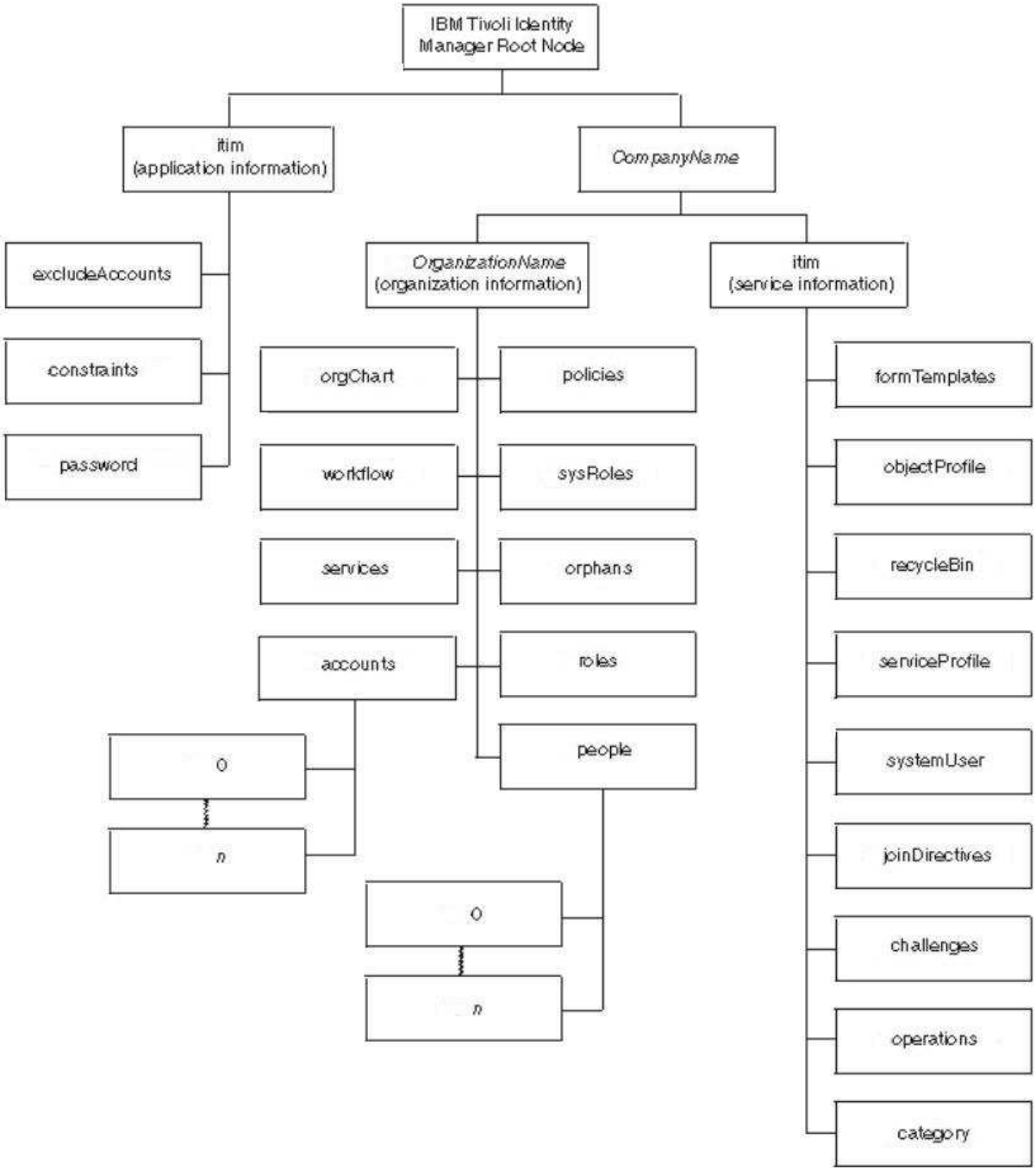
Quando un'azienda o in questo caso strutture pubbliche cominciano a mettere a disposizione risorse alle sue organizzazioni interne, deve essere implementato un sistema di autoregolamentazione della gestione degli account, che realizzi i vantaggi e i benefici del provisioning degli utenti. In questo ambiente un cambiamento di stato di un utente si riflette automaticamente sui diritti di accesso che questo ha alle risorse interne. E' possibile ridurre i costi di provisioning, snellire gli accessi e i processi di approvazione, potendo così sfruttare il pieno potenziale di un sistema di controllo degli accessi basato sui ruoli. Inoltre è possibile ridurre i costi di amministrazione attraverso procedure automatizzate per la gestione del provisioning degli utenti, migliorando la sicurezza, automatizzandone le politiche di rinforzo, e snellendo e centralizzando la gestione del ciclo di vita utente e le risorse di provisioning per una vasta popolazione di utenti.

PERSONALIZZAZIONE

Il livello di personalizzazione di questo pacchetto viene scelto dal team di progetto a seconda della dimensione della struttura su cui si vorrà implementarlo. Ovviamente strutture od aziende di grandi dimensioni per esempio richiederanno un piano di personalizzazione più complesso rispetto ad una piccola azienda con tempistiche più lunghe. Nel nostro caso questo deve essere installato in tutte le sedi dislocate nel territorio comunale quindi ipotizziamo una personalizzazione standard per ognuna di queste con piccole differenze riguardo ai vari livelli di sicurezza

4.5.3. Basi di dati

I dati che devono essere memorizzati consistono nelle informazioni personali di ciascun utente il quale deve avere un' identificativo univoco all'interno del sistema. Il metodo di assegnazione dello UserID avviene tramite un algoritmo che può essere scelto dagli amministratori. La base di dati deve contenere poi anche i diritti di ciascun utente ossia quelle regole in grado di specificare a quali informazioni ed a quali applicazione l'utente avrà libero accesso.



Schema della strutturazione dei dati nel sistema di Identity Manager di IBM

Contenuto	Descrizione
Root Node	Nodo principale dove Tivoli Identity Manager Server è installato
Itim	Contiene tutte le informazioni pertinenti utili per Tivoli Identity Manager
Constraints	Contiene i diritti di accesso per gli utenti per varie regole e servizi
Password	Contiene le password invalide inserite
CompanyName	Nome della società, contiene tutte le informazioni riguardanti
OrganizationName	Nome dell'organizzazione che comparirà nell'albero organizzativo
orgChart	Contiene la definizione dell'organizzazione
Workflow	Contiene tutti i workflow per essere utilizzati all'interno del sistema di Identity Managment
Services	Contiene le informazioni riguardanti i servizi installati
Accounts	Contiene tutti gli account presenti nel sistema
Policies	Contiene tutte le politiche definite
sysRoles	Contiene tutte le regole definite per la gestione del sistema
Orphans	Contiene tutti gli account orfani trovati durante un controllo
Roles	Contiene tutte le informazioni sulle regole per la gestione degli account
People	Contiene tutte le informazioni personali degli utenti
Itim	Contiene,similarmente al precedente,informazioni specifiche di sistema
formTemplates	Contiene informazioni a riguardo di vari form che vengono utilizzati
objectProfile	Contiene profili di oggetti richiesti dal sistema per riconoscere e gestire le risorse
recycleBin	Contiene le entità eliminate dal sistema utilizzando l'interfaccia grafica
serviceProfile	Contiene i profili di servizio richiesti dal sistema per riconoscere e gestire le risorse come un servizio
systemUser	Contiene informazioni a riguardo degli utenti di sistema
joinDirectives	Contiene tutte le informazioni sulla politica di provisioning
Challenges	Contiene tutte le informazioni riguardo l'autenticazione attraverso password richesta/risposta
Operations	Contiene le informazioni sule operazioni con i workflow (come aggiunte, modifiche, cancellazioni, sospensioni e rasferimenti)
Category	Contiene le operazioni di gestione del ciclo di vita per ogni tipo di entità. Solo persone e account sono supportate. E' possibile indicare un operazione di sistema

Tabella della descrizione di tutti i vari componenti che identificano i dati nel sistema

Il volume della base di dati è quindi proporzionale al numero di utenti che utilizzano il sistema. Quando uno di questi viene aggiunto viene inserito anche all'interno della base di dati assegnandogli a seconda delle politiche di provisioning l'accesso a informazione e ad applicazioni.
La base di dati viene aggiornata qualora ci siano delle modifiche ai dati personali dell'utente. Nel caso di modifiche riguardanti il ruolo ricoperto all'interno delle strutture si ha una conseguente modifica dei diritti di accesso, o ancora quando avvengono modifiche riguardanti le politiche di accesso esse prevedendo la modifica delle concessione degli accessi ad una parte od alla totalità delle utenze.

4.5.4. Componenti tecnologiche

Componenti hardware:

La scelta del server è ricaduta su una soluzione IBM che è stata considerata la migliore valutandone il rapporto prezzo/prestazioni, ha la possibilità di scelta del processore fra dual core o quad core. In base alle esigenze del sistema optiamo per una cpu con soli 2 core limitandone così anche il costo.

IBM Server x3200 M2

Caratteristiche principali:

- Gestione della crescita e dei rischi con configurazioni flessibili, protezione dei dati e prestazioni applicative
- Controllo della complessità con opzioni di gestione integrata e remota
- Funzioni standard garantiscono alti livelli di disponibilità del sistema

Principali caratteristiche hardware:

- Formato tower montabile in rack
- Possibilità di scelta del processore – Intel Xeon quad-core o dual-core
- Fino a 2 GB di memoria standard e 8 GB di memoria massima DDR III a 1600 o 1800 MHz
- Opzioni storage flessibili – fino a quattro unità SATA (Serial Advanced Technology Attachment) simple-swap o hot-swap da 3,5 pollici, quattro unità SAS (Serial Attached SCSI) hot-swap da 2,5/3,5 pollici o otto unità SAS hot-swap da 2,5 pollici
- Fino a 1,17 TB di capacità massima con otto unità disco fisso SAS da 2,5 pollici o fino a 4,0 TB di capacità massima con quattro unità disco fisso SATA da 3,5 pollici

- Modello con alimentatori ridondati hot-swap
- Combinazione di unità ottiche DVD-ROM/ CD-RW
- RAID hardware -0 e -1 senza slot integrato per una migliore protezione dei dati (in base al modello) – upgrade opzionale al supporto RAID-5
- Mini-BMC2 integrato con supporto IPMI 2.0
- RSA (Remote Supervisor Adapter) II SlimLine opzionale
- Opzioni di backup su nastro interne

WD ShareSpace WDA4NC40000

Caratteristiche principali:

- *Affidabilità:* l'elevata disponibilità dei dati e le funzioni di ridondanza a livello di sistema consentono di rispondere efficacemente alle esigenze di applicazioni business-critical e mission-critical
- *Versatilità:* una singola architettura integrata supporta l'I/O (Input/Output) di block concorrenti e il file serving su infrastrutture SAN (Storage Area Network) Ethernet e Fibre Channel (FC)
- *Velocità:* supporto di throughput elevati e tempi di risposta rapidi per applicazioni di database, di e-mail e tecniche
- *Flessibilità:* le funzionalità delle unità a disco FC e SATA (Serial Advanced Technology Attachment) permettono l'implementazione in ambienti a più soluzioni, inclusi i processi di conservazione dei dati per conformità alle normative, storage nearline, backup disk-to-disk e operazioni mission-critical ad elevato I/O caratterizzate da alte prestazioni.

Principali caratteristiche hardware:

- Fino a 8 TB di capacità storage
- Una porta a 1 Gbps
- Porta LVD SCSI
- LED/LCD di diagnostica
- Due ventole di raffreddamento e due alimentatori auto-ranging hot-plug ridondati integrati

Componenti del sotware applicativo:

Il pacchetto software con struttura modulare è composto dalle seguenti parti:

- Tivoli Identity Manager
- Tivoli Access Manager
- Tivoli Federated Identity Manager

Tutti questi moduli sono necessari per l'autenticazione degli utenti e l'accesso alle risorse ed assicura che l'accesso sia in loco coerentemente applicato.

Descrizione di ciascun modulo:

Tivoli Identity Manager

Fornisce un sicuro e automatizzato sistema di gestione degli account utente basato su politiche di accesso che aiuta a gestire efficientemente le identità dell'utente attraverso tutto il loro ciclo di vita negli ambienti di e-business. Fornisce un accesso centralizzato alle diverse risorse, mediante politiche e caratteristiche che snelliscono le operazioni associate con l'accesso alle risorse utente. Come risultato si godrà di vari benefici tra i quali:

- Web self service, reset delle password e sincronizzazione; gli utenti possono auto amministrarsi le password utilizzando le regole delle politiche di gestione delle password per controllare l'accesso a più applicazioni. La sincronizzazione delle password permette agli utenti di usare una password per tutti gli account che Tivoli Identity Manager gestisce.
- Rapida risposta ai controlli e ai mandati di regolamentazione
- Automazione dei processi correlati alle modifiche delle identità dell'utente con l'uso di una gestione del suo intero ciclo di vita
- Controllo centralizzato e autonomia locale
- Una migliore integrazione con l'uso delle APIs estese
- Possibilità di scelta se gestire sistemi target con approccio senza agente o con agente
- Aumento della sicurezza degli accessi attraverso la riduzione degli account orfani

Tivoli Access Manager

Permette alle varie strutture l'uso centralizzato delle politiche di sicurezza per uno specifico gruppo di utenti gestendo le autorizzazioni d'accesso attraverso la rete includendo quelle vulnerabili. Può essere strettamente legato con Tivoli Identity Manager per mettere insieme gruppi di utenti e account gestiti da Tivoli Access Manager con le identità gestiste

dall'Identity Manager fornendo una soluzione integrata per il controllo dell'accesso alle risorse.
Tivoli Access Manager offre:

- Unificazione degli accessi di autenticazione e autorizzazione con le diverse applicazioni basate su Web
- Single sign-on flessibile da ambienti Web, Microsoft, telnet e applicazioni mainframe
- Rapido e scalabile schieramento di applicazioni Web, con supporti standard per applicazioni basate su Java™ 2 Enterprise Edition (J2EE)
- Flessibilità di progettazione attraverso un'architettura proxy di elevata scalabilità e Web server plug-ins facili da installare, controllo degli accessi basato su regole e ruoli, supporto per guidare la registrazione degli utenti e delle platforms, APIs avanzate per la personalizzazione della sicurezza

Tivoli Federated Identity Manager

Gestisce tutte le informazioni di configurazione in tutti i suoi confini, inclusi i rapporti con i partner, mappatura delle identità e gestione delle identità token.
Tivoli Federated Identity Manager consente di condividere servizi con i business partner dell'ente ottenendo informazioni affidabili da identità di terze parti come, "clienti", fornitori, e dipendenti delle diverse sedi. E' possibile ottenere informazioni senza dover creare, iscrivere, o gestire account di identità con le aziende che forniscono l'accesso ai servizi che sono usati all'interno delle strutture. Di conseguenza gli utenti sono risparmiati dal dover registrarsi sul sito dell'azienda partner e dal dover ricordarsi di login aggiuntivi e password. Il risultato è una migliore integrazione e comunicazione con i suoi fornitori, business partner e clienti.

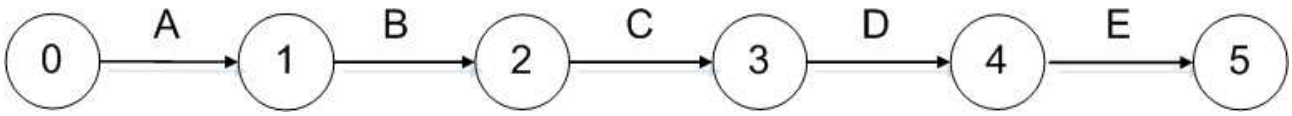
4.5.5. Linee guida

Il sistema necessita di interventi manutentivi periodici, poiché deve venire assicurata l'efficienza e la funzionalità del sistema. Possono essere previsti degli interventi su software dovuti a modifiche ad esempio a vincoli normativi i quali impongono il cambiamento di un parte del sistema. La flessibilità di questo software permette di eseguire le modifiche senza dover interpellare la ditta produttrice.
I dati contenuti all'interno del database devono essere soggetti a copie di back-up per eliminare eventuali possibilità di perdita degli stessi.
Esistono diverse strategia di back-up dei dati, la prima innanzitutto viene implementata all'interno del NAS stesso impostando i dischi in modalità raid-1, ovvero vi sono

informazioni ridondanti, cioè, vi sono 2 o più copie dello stesso hard disk. In questo modo anche se vi è un danneggiamento ad un hard disk è possibile recuperare i dati all'interno dell'altro hard disk contente l'intera copia di quello danneggiato. E' possibile inoltre la cosiddetta sostituzione a caldo "hot swap" dell'HD senza dover arrestare il sistema mantenendo cosi sempre la disponibilità dei dati.
Il sistema raid-1, oltre a garantire la disponibilità dei dati ne aumenta anche le prestazioni in lettura, grazie alla presenza di più copie è possibile la lettura in parallelo degli stessi con una conseguente diminuzione del tempo di accesso.
Periodicamente sarà necessario effettuare una copia di back-up vera e propria all'interno di un supporto di memorizzazione che può essere ottico come un dvd o su nastro magnetico.
A ciascuno di questi back-up completi con i quali è possibile ripristinare l'intero sistema solitamente si associano alcuni back-up incrementali non consistenti, questi sono back-up parziali che da soli non sono in grado di ripristinare il sistema ma che aggiunti al predente back-up completo riescono a riportare il sistema più vicino possibile alla situazione esistente prima che si verificasse il guasto.

4.5.6. Piano di realizzazione

Per evidenziare le fasi di realizzazione riportiamo il diagramma CPM che evidenzia la successione temporale delle varie fasi:



A) Acquisto del prodotto e personalizzazione;
B) Installazione;
C) Migrazione dati;
D) Formazione utenti;
E) Periodo di prova.

Il tempo necessario per l'acquisto, la personalizzazione e l'installazione del prodotto è dovuto principalmente al tempo impiegato per rendere più adatto il software a quelle che sono le esigenze dell'ente cercando di adattare al meglio il sistema per tutte le sedi del cliente dislocate nel territorio e per renderne possibile l'iterazione tra di loro. La personalizzazione ad esempio viene applicata se si pensa che sedi bisogno di livelli di sicurezza diversi di accesso ai dati, differenti tra biblioteca e asilo nido. Si dovrà comunque garantire la possibilità di comunicazione e di scambio di informazioni tra di loro.

Per quanto riguarda la formazione degli utenti avviene in cinque giorni, o meglio questi vengono suddivisi in 2 giorni dedicati alla formazione del personale tecnico per l'installazione del sistema ed ulteriori 3 giorni per la formazione degli utenti affinché questi possano utilizzare il sistema sfruttandone al massimo le sue potenzialità.
Infine si avrà una fase di avviamento in parallelo al sistema che veniva utilizzato in precedenza per rilevarne eventuali errori ed anomalie e per poter procedere eventualmente alla correzione dei bug rilevati. Questa fase di avvio in parallelo occupa circa 180 giorni.
Il totale quindi i giorni per rendere operativa questa soluzione è di 365 giorni lavorativi contando la formazione sia del personale tecnico che degli utenti.

4.5.7. Aspetti organizzativi

Interventi ai processi:

La realizzazione del sistema di identity management comporta un reale cambiamento al modus operandi fin'ora adottato. Innanzitutto tutte le operazioni che prima venivano eseguite su carta come la registrazione di un nuovo impiegato e dei suoi relativi dati viene ora eseguito a computer, alla fine della quale verrà creato un nuovo account con assegnato il ruolo che ricopre il nuovo utente e i relativi privilegi.
Inoltre tutte le operazioni di accesso ai dati saranno ora per via telematica. Non ci sarà più bisogno di particolari autorizzazioni firmate dai responsabili per poter accedere ai documenti del tipo progetti, schemi, tabelle di codici o altro, il controllo della effettiva possibilità di reperire informazioni sensibili riguardanti le varie strutture verrà ora automaticamente verificato dal sistema dopo aver effettuato la procedura di login.
Quindi tutte quelle operazioni che richiedevano delle autorizzazioni per compiere una qualsiasi attività come ad esempio la formale richiesta delle ferie o l'invio di un certificato medico o ancora la timbratura del cartellino verranno eseguite e controllate in modo automatico e inoltrate direttamente a quelle figure le quali hanno il potere di poter accettare, modificare o rifiutare tale richiesta.

Interventi alle strutture:

Il lavoro della segreteria e della gestione da parte dell'IT di tutte quelle informazioni dell'utente, i permessi, le buste paga ecc. saranno ora compiti del sistema che provvederà all'immagazzinamento e alla loro verifica. Quindi sarà necessario l'acquisto di server per poter far lavorare il sistema, con una buona quantità di memoria per l'immagazzinamento dei dati, inoltre saranno necessari dei client da disporre all'interno delle varie strutture con relativo

lettore di badge che servirà ai vari utenti per autenticarsi ed accedere ai propri dati sensibili e alle risorse e servizi che gli permettano di svolgere il proprio lavoro. Gli amministratori di sistema avranno la possibilità di accesso assoluto per poter controllare e modificare il sistema in base alle proprie esigenze. Per quanto riguarda la rete interna non ci saranno modifiche importanti se non per ciò che riguarda la configurazione dei client e dei server.

Interventi di formazione:

Quanto detto comporta sicuramente un cambiamento nell'organizzazione. Il personale che sarà responsabile del sistema andrà formato con i relativi corsi che saranno tenuti in sede da tecnici qualificati con un'alta conoscenza del software. La formazione dei dipendenti prevederà un training per l'utilizzo del sistema della durata di 3 giorni ai quali vanno aggiunti altri 2 giorni per l'installazione del sistema eseguito da un tecnico specializzato.

Necessità di supporto al sistema a regime (risorse tecniche informatiche):

Per il mantenimento e la manutenzione sono necessari due tecnici informatici che saranno formati per poter gestire e risolvere eventuali problemi al sistema. Durata dei corsi prevista per la formazione 2 giorni.

4.5.8. Gestione del rischio

Da quanto emerge dall'analisi effettuata, i rischi che si corrono sono di entità medio-bassa visto anche che si tratta di software già in uso in varie aziende.
I tempi di messa in esercizio del sistema dipendono da scadenze non modificabili imposte dai fornitori (ma regolate da vincoli contrattuali); è da considerare tuttavia che i tempi previsti sono ampiamente inferiori a quelli imposti dai vincoli temporali.
Anche i costi previsti sono inferiori a quelli imposti dai vincoli economici.

4.5.9. Analisi dei benefici

I benefici *interni* dovuti a *maggiore efficienza* sono i seguenti:

- Riduzione del personale addetto all'help desk
- Riduzione del tempo di attesa in caso di smarrimento password

I benefici *interni operativi* sono i seguenti:

- Aumento della sicurezza
- Riduzione dei costi amministrativi attraverso il supporto automatizzato degli utenti

- Riduzioni del costo di Help Desk
- Riduzione dei costi e dei ritardi associati all'accesso dell'approvvigionamento delle risorse con un nuovo e miglior utente

I benefici *interni strategici* sono i seguenti:

- Gestione ottimizzata della carriera di ciascun utente con assegnazione di privilegi a seconda del ruolo ricoperto

Riduzione del personale addetto all'help desk:

Eliminazione delle chiamate ricevute agli help desk da parte degli utenti per problemi correlati alle password. Fare in modo che gli utenti possano modificare le password e gestire le loro identità nel rispetto delle norme interne e liberare l'help desk da questo carico di lavoro. Quando un utente dimentica la propria password, non è più necessaria l'iterazione con l'help desk perché ci si potrà servire di un'apposita applicazione per il reset automatico. Inoltre molte procedure prima eseguite manualmente ora sono automatizzate dal software grazie anche ad un efficiente sistema di reportistica . E' possibile quindi una diminuzione del personale dovuta alla diminuzione del carico del lavoro.

Riduzione del tempo di attesa in caso di smarrimento password:

Solitamente un dipendente che dimentica la propria password deve chiamare l'help desk per richiederne il ripristino, perdendo tempo prezioso e aumentato i costi del supporto. Il sistema consente di sincronizzare le password degli utenti fornendo un'unica password per tutti i sistemi, che sarà più facile da ricordare (SSO single sign-on).
Se un utente dimentica la propria password, entra in gioco l'applicazione utente, che consente di creare, modificare e ripristinare la password senza chiamare l'help desk e rubare il suo tempo.

Aumento della sicurezza:

L'uso di un sistema di gestione automatizzato delle regole di accesso e delle autorizzazioni fa si che la sicurezza degli accessi sia sempre garantita, grazie anche alla possibilità di personalizzazione attraverso APIs fornite dal programma. L'implementazione di una nuova gestione dei pericolosi account *orfani* permette di avere maggior sicurezza e controllo sugli accessi eliminando possibili punti deboli del sistema. Inoltre permette alle strutture di essere sempre conformi alle leggi e norme che regolano il trattamento dei dati.

Riduzione dei costi amministrativi attraverso il supporto automatizzato degli utenti

Con l'uso di un sistema centralizzato con punto singolo locale d'accesso non ci sarà più bisogno di tediose pratiche burocratiche per la registrazione e la gestione dei dati degli utenti da parte dell'amministrazione dei sistemi. L'automatizzazione di questi meccanismi permette una riduzioni dei tempi e quindi uno svolgimento del lavoro più snello con una conseguente riduzione dei costi. Infine saranno gli utenti stessi ora a eseguire l'inserimento dei propri dati grazie ad un supporto automatico che guiderà l'utente nella sua registrazione e nella gestione dei suoi criteri d'accesso che verranno poi controllati dagli amministratori di sistema per la conferma della veridicità.

Riduzioni del costo di Help Desk

Se dovesse insorgere un problema al sistema, questo verrà immediatamente notificato agli amministratori competenti senza dover essere smistato fra i vari componenti dello staff. Il tecnico competente per quel determinato settore riceverà notifica di un malfunzionamento del sistema e provvederà immediatamente a risolverlo in base anche ad un sistema che ne assegna vari valori di criticità al problema. Non ci saranno più quindi notifiche tramite telefonate o e-mail all'help desk che a sua volta doveva interpellare chi di dovere. Riduzione quindi del personale addetto all'help desk con diminuzione conseguente del costo e dei tempi.

Riduzione dei costi e dei ritardi associati all'accesso dell'approvvigionamento delle risorse con un nuovo e miglior utente

Il nuovo sistema permette un diretto contatto con gli eventuali fornitori attraverso un processo di autenticazione sicuro ed affidabile che tiene inoltre traccia di tutte le transazioni eseguite e del loro stato. Ottenere informazioni e gestire gli ordini sarà molto più semplice e veloce e non saranno più necessarie lunghe registrazioni sui siti dei fornitori. Gli ordini quindi per le forniture delle risorse verranno inoltrate in tempo reale al fornitore che provvederà quanto richiesto.

Gestione ottimizzata della carriera utente con assegnazione di privilegi a seconda del ruolo ricoperto:

Nel corso della loro carriera professionale all'interno di un'organizzazione i dipendenti/utenti possono ricoprire più di un ruolo. Il programma consente di gestire automaticamente e in sicurezza le esigenze di accesso degli utenti, anche quando i ruoli cambiano e vengono

assegnate nuove responsabilità od autorizzazioni. A tale scopo viene creata un'area di autorizzazioni che consente di definire e gestire le norme di autorizzazione basate sui ruoli. Queste norme assegnano autorizzazioni a gruppi specifici di utenti per appartenenze. Inoltre viene gestito il caso in cui, ad esempio, l'utente modifichi il suo ruolo in "licenziato" nel qual caso viene bloccato l'accesso a tutte le informazione ed a tutti i sistemi, per evitare spiacevoli inconvenienti che potrebbero provocare la perdita e l'accesso non autorizzato ad informazioni contenute all'interno del sistema.

4.5.10. Valutazione dei costi

Costi per l'hardware

Sono stati valutato nella tabella sottostante i costi per l'acquisto dell'hardware:

Prodotto	Prezzo	Quantità	Prezzo totale
WD ShareSpace_WDA4NC40000	760.00€	1	760.00€
Server IBM System x3200 M2	1150.00€	1	1150.00€
Lettori di badge	55.00€	51	2805.00€
Aggiornamenti a PC che non soddisfano requisiti minimi	130.00€	38	4940.00€
COSTO TOTALE			9655.00€

Tabella relativa alla valutazione del costo dell'hardware

Costi di Progetto

Costi totali per la creazione del progetto, in questa tabella sono riportate alcune voci quali: acquisizione che sono i costi per la redazione della documentazione di progetto; le licenze dei PC sono state rinnovate a quei computer che avevano installato un sistema operativo diventato ormai obsoleto e quindi è stata necessaria la sostituzione; il costo poi del pacchetto applicativo viene diviso in server e client quest'ultimo varia a seconda della quantità dei client che ne faranno uso. Il costo per la migrazione dati è stato calcolato ipotizzando il lavoro di una persona per 3 mesi ad 900€/mese, dati prima contenuti all'interno di vari database.

Prodotto	Prezzo	Costruzione/ avviamento	Interni / esterni
Progettazione	1000.00€	costruzione	Esterno diretto
Acquisizione	200.00€	costruzione	Esterno diretto
Hardware	9655.00€	costruzione	Interno indotto
Software di base			
Licenze per i pc che non ne sono in possesso	6450.00€	costruzione	Esterno indotto
Software d'ambiente	0 €	----------	----------
Software applicativo			
Server	3141.60€	costruzione	Esterno diretto
Client (24.00€ x 80)	1920.00€	costruzione	Esterno diretto
Costituzione delle banche dati	2750.00€	costruzione	Interno indotto
Formazione	1476.00€	avviamento	Interno indotto
Avviamento	1590.00€	avviamento	Interno diretto
COSTO TOTALE	**28182.60€**		

Costi di Gestione

Costi dovuti alla gestione del nuovo sistema preso in esame, questi si caratterizzano per un costo di assistenza annua da parte di IBM che nel primo anno è compresa nel prezzo di acquisizione del pacchetto e da un costo del personale amministrativo da considerarsi per singola persona.

Prodotto	Prezzo	Esercizio/ manutenzione
Assistenza agli utenti da parte di IBM (contratto annuo) dopo il primo anno	10000.00€	Esercizio
Rinnovo licenze	5000.00€	Esercizio
Costo personale amministrativo (2 persone, prezzo da riferirsi a singola persona)	12000.00€	Esercizio
Costo materiali di consumo	300.00€	Esercizio
Costi energetici	250.00€	Esercizio
Costi per le comunicazioni	2000.00€	Esercizio
Costo manutenzione hardware	1500.00€	Manutenzione
Aggiornamento dei dati	100.00€	Manutenzione
COSTO TOTALE	**43150.00€**	

4.5.11. Analisi costi/benefici

Costi attualmente sostenuti:

Nella tabella sono riportati i costi che sono sostenuti attualmente dall'ente per la gestione del sistema, la principale differenza è la presenza di 4 persone lo svolgimento delle funzioni di help desk, questo provoca un evidente aumento del costo annuo di gestione.

Prodotto	Prezzo	Esercizio/ manutenzione
Rinnovo licenze	5000.00€	Esercizio
Costo personale amministrativo (4 persone, prezzo da riferirsi a singola persona)	15000.00€	Esercizio
Costo materiali di consumo	1500.00€	Esercizio
Costi energetici	250.00€	Esercizio
Costi per le comunicazioni	2000.00€	Esercizio
Costo manutenzione hardware	1500.00€	Manutenzione
Aggiornamento dei dati	100.00€	Manutenzione
COSTO TOTALE	**70550.00€**	

Tempistica di progetto:

Tempi previsti per il progetto:

Costi	Durata
Consegna / installazione	3 mesi
Migrazione dati	3 mesi
Formazione degli utenti	5 giorni
Avviamento in parallelo	6 mesi

Tabella per il calcolo del periodo di pay-back:

Nella tabella seguente analizziamo i costi annui sostenuti dalla situazione esistente e dal progetto in esame. Si considera che il costo sostenuto nel primo anno dal progetto è superiore a quello della situazione esistente ma nel corso del tempo si arriva ad un punto in cui il costo del nuovo progetto risulta inferiore rispetto alla soluzione attuale, quello è considerato come il punto di break even point.

Anno	Costi Attuali	Costi progetto
1	**70550.00**€+	28182.60€ + 33150.00€ + 70550.00€ =
		131882.60€ +
2	70550.00€=	43150.00 =
	141100.00€ +	**175032.60**€ +
3	70550.00€=	43150.00€ =
	211650.00€ +	**218182.60**€ +
4	70550.00€=	43150.00€ =
	282200.00€	**261332.60**€

5.CONCLUSIONI

Nella realizzazione di questo studio di fattibilità di un sistema di Identity Management siamo andati a valutare le proposte delle migliori aziende che producono software analizzandone poi le differenze anche in base a diverse tipologie di soluzione. Una delle prime modalità di realizzazione che abbiamo a scartato è stata quella di tipo In-house perché evidentemente l'ente non dispone di uno staff e di una struttura adeguata a realizzare questo tipo di soluzione.

Proseguendo poi nell'analisi delle rimanenti soluzioni ci siamo scontrati con l'impossibilità di realizzare la proposta di Oracle a causa dei vincoli economici che ci erano stati imposti. Altra modalità che non rispettava i vincoli di tipo economico era la soluzione con commessa esterna, che richiedeva inoltre un tempo di realizzazione molto più lungo, dato ovviamente dalla creazione da zero del software.

Tra le proposte quindi rimaste abbiamo trovato dei validi software che soddisfano in maniera ottimale le esigenze dell'ente. Fra i quali anche un software di tipo Open Source che prometteva dei risultati molto buoni pur essendo in libera licenza, ma che non si adattava bene al nostro progetto non potendo fornire un sicuro supporto al nostro cliente.

Quindi dopo un'attenta analisi del rischio una sola delle ipotesi si è rivelata vincitrice. Infatti l'offerta di IBM è stata una soluzione che ci ha permesso di rispettare tutti i vincoli progettuali mantenendo degli ottimi margini di sicurezza soprattutto per quanto riguarda i tempi della messa in opera e dei costi totali. Procedendo con il progetto per sola questa ipotesi si può ricavare come non solo sia risultata la migliore fra tutte ma anche riesca ad offrire servizi che non ci erano stati richiesti ma che posso essere comunque sfruttati per godere al massimo delle potenzialità di questo software.

Come ci veniva richiesto inoltre l'automatizzazione di molti processi permette la riduzione del personale IT e l'aumento notevole della sicurezza dei dati del sistema. Accedere ora alle informazioni, applicazioni e risorse interne sarà più semplice, intuitivo e soprattutto veloce e comodo grazie all'utilizzo di client disposti in più punti all'interno delle varie strutture. Anche le stesse comunicazioni fra le varie sedi sarà semplificata mantenendo comunque un alto livello di sicurezza per lo scambio delle informazioni.

Ma cosa più importante sono i costi. Questo nuovo sistema infatti permette dopo solo circa 3 anni e 4 mesi di raggiungere il punto di pay-back. Da quel momento in poi il cliente ne trarrà solo dei benefici in termini economici con un notevole risparmio nel tempo di denaro. Infatti

il costo di manutenzione grazie anche alla riduzione del personale amministrativo è notevolmente ridotto con possibilità di investimento in altri settori. I dati con questa soluzione sono organizzati in un unico database e risultano quindi di più facile reperimento, manutenzione e sicuri da accessi non consentiti.